Trabajo de fin de grado

Universidad de Murcia

Facultad de Matemáticas

CURVAS ELÍPTICAS

Autor:
Sara N. Matheu García

Supervisor:
Dr. Ángel del río mateos

22 de junio de 2015

Algebrista te volviste
refinado hasta la esencia
oligarca de la ciencia
matemático bacán.

Hoy mirás a los que sudan
en las otras disciplinas
como dama a pobres minas
que laburan por el pan.

¿Te acuerdas que en otros tiempos
sin mayores pretensiones
mendigabas soluciones
a una mísera ecuación?

Hoy la vas de riguroso
revisás los postulados
y junás por todos lados
la más vil definición.

Pero no engrupís a nadie
y es inútil que te embales
con anillos, con ideales
y con álgebras de Boole.

Todos saben que hace poco
resolviste hasta matrices
y rastreabas las raíces
con el método de Sturm.

Pero puede que algún día
con las vueltas de la vida
tanta cáscara aburrida
te llegue a cansar al fin.

Y añores tal vez el día
que sin álgebras abstractas
y con dos cifras exactas
te sentías tan feliz.

Enzo R. Gentile

Índice general

Índice de figuras

Índice de tablas

Resumen

El objetivo del presente trabajo es estudiar los fundamentos matemáticos sobre los que se basan las curvas elípticas. Aunque se introducen definiciones nuevas, la mayoría de ellas derivan de conceptos vistos en las asignaturas de Ampliación de Álgebra Lineal y Geometría, Grupos y Anillos y Ecuaciones Algebraicas, luego cualquier estudiante debería ser capaz de entender este documento con relativa facilidad. Sin embargo, como el álgebra no deja de ser abstracta, para facilitar el entendimiento se ha intentado refrescar todos esos conceptos que pueden estar un poco olvidados en nuestra memoria, antes de pasar a definir otros nuevos.

El estudio de las curvas elípticas no es un tema realmente nuevo. Las curvas elípticas han ocupado un papel central en matemáticas desde hace tres siglos y sus notables propiedades aritméticas y geométricas han encontrado aplicación en múltiples problemas y campos matemáticos. Su empleo en criptografía es sin embargo reciente, pudiéndose situar su inicio en el año 1985, gracias a Miller[1] y Koblitz[2].

La criptografía es la ciencia encargada del estudio y diseño de sistemas que permiten ocultar información. Desde sus inicios, esta capacidad de encubrimiento se ha basado en la dificultad que supondría a una entidad no autorizada obtener la información original en un conjunto de datos cifrado. Actualmente, en tiempos donde el avance tecnológico en la informática y las telecomunicaciones es cada vez mayor, donde se estima que cada día Google procesa cerca de 25 petabytes de datos, que Facebook comparte más de 10 millones de fotografías y que en Youtube se sube una hora de vídeo cada segundo, la criptografía se ha hecho indispensable. Las cuentas de correo electrónico, las redes sociales, las transacciones bancarias por cajero electrónico o a través de Internet, entre muchos otros, están protegidos mediante criptosistemas, es decir, un conjunto de procedimientos que garantizan la seguridad de la información. Es así como el uso de la criptografía, aún sin saberlo la mayoría de las personas, se ha convertido en una realidad del día a día.

Otro campo de la tecnología también crece: El Internet de las cosas o Internet-of-Things (IoT), que es la a unión de los objetos físicos y la electrónica, software, sensores y conectividad para que pueda lograr un mayor valor y servicio a través del intercambio de datos con el fabricante, operador y/u otros dispositivos conectados. Cada uno de esos objetos es capaz de interoperar en la infraestructura actual de Internet. Ya existen lavadoras con WiFi, neveras que saben los alimentos que contienen y te preparan la lista de la compra, lámparas que saben cuando tienen que encenderse, etc. En un futuro no muy lejano todos los objetos comunes de nuestra casa y ciudad podrán disponer de conexión a Internet, facilitándonos su gestión a distancia desde el portátil, la tablet o incluso el móvil. Obviamente, todas estas conexiones necesitan ser protegidas, que es de lo que se encarga la criptografía. Sin embargo, estos pequeños dispositivos no son ordenadores convencionales, en el sentido de que no tienen una gran potencia de cálculo, una gran memoria RAM o un gran disco duro.

La criptografía se suele dividir en criptografía simétrica y asimétrica. Los algoritmos simétricos se caracterizan por el uso de una misma clave para cifrar y descifrar. Ambas partes (emisor y receptor) deben conocer la clave de antemano. Estos algoritmos son rápidos y son los que se usan para cifrar nuestros mensajes. Por contra, los algoritmos asimétricos disponen de dos claves, una pública que se utiliza para cifrar y que está disponible para cualquiera que desee utilizarla

[1] V. Miller: Use of elliptic curves in Cryptography, 1985
[2] N. Koblitz: Elliptic Curve Cryptography, 1987

y otra privada que se utiliza para descifrar. Estos algoritmos son más lentos y necesitan claves más grandes, pero son necesarios para poder suministrar una clave simétrica a ambas partes de la comunicación.

Actualmente uno de los protocolos criptográficos asimétricos que más se utilizan es RSA. El problema es que cada vez es se necesitan claves más grandes, ya que la potencia de cálculo de los ordenadores se va incrementando día a día, y una clave pequeña puede ser descifrada fácilmente. ¿Qué pasará cuando las claves que cifran nuestros datos sean tan grandes que no puedan ser procesadas en esos pequeños dispositivos de los que hablábamos? Una posible solución es el uso de protocolos criptográficos con curvas elípticas. En aquellas aplicaciones que requieren un nivel de seguridad bastante elevado (con lo cual, la longitud de las claves aumenta considerablemente), la criptografía de curvas elípticas puede proporcionar el nivel de seguridad parecido destinando menos recursos para conseguirlo. Esto significa que su uso en esos dispositivos limitados puede proporcionar un nivel de seguridad muy elevado sin necesidad de incrementar su coste de producción. Actualmente, existen empresas que están realizando estudios de curva elíptica en plataformas como MBED [29].

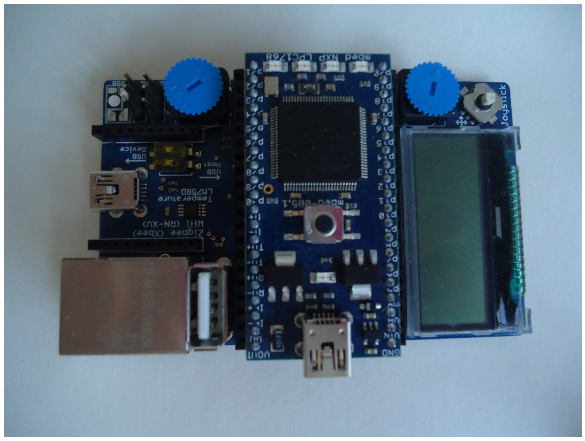

Figura 1: MBED Córtex M3

Para conocer la base matemática de este tipo de criptografía, necesitaremos comenzar en el Capítulo 1, Sección 1.1 recordando y ampliando nuestros conocimientos de cuerpos finitos $\mathbb{F}_q$ de un determinado orden q, ya que las curvas elípticas se van a definir sobre un cuerpo finito. También repasaremos el espacio afín y proyectivo en la Sección 1.2 porque para representar los puntos de dicha curva, utilizaremos las llamadas coordenadas homogéneas del espacio proyectivo, que nos permitirán tratar a los puntos del infinito como puntos cualesquiera. En este capítulo veremos conceptos nuevos como los puntos singulares, los puntos de inflexión, y el más importante de todos: el orden de intersección. El orden de intersección puede definirse tanto en el espacio afín como en el proyectivo y en este capítulo veremos que este concepto está bien definido, es decir, siempre existe, y estudiaremos una serie de propiedades interesantes para poder manipularlo mejor.

Una vez que tenemos todos los conceptos básicos asimilados, en el Capítulo 2 definiremos al fin lo que es una curva elíptica. Veremos dos maneras de presentarla, una más general, la ecuación general de Weierstrass,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

y una más sencilla para cuerpos con característica distinta de dos y tres, la ecuación simplificada de Weierstrass,

$$y^2 = x^3 + Ax + B,$$

donde todos los coeficientes se toman en el cuerpo fijado para la curva elíptica.

Sabiendo ya lo que es una curva elíptica, definiremos la operación de suma de puntos en la Sección 2.2 de la siguiente manera: Si tenemos dos puntos P, Q pertenecientes a una curva elíptica podemos trazar la recta que contiene a P y Q (si $P = Q$, será la recta tangente). Esta recta cortará a la curva en un tercer punto R. Definiremos $P + Q = -R$ como el simétrico de R con respecto al eje x.

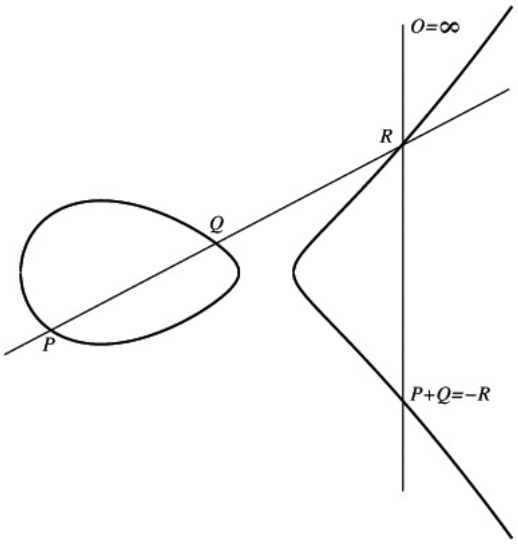

Figura 2: Suma de puntos. **Fuente**: [7]

Veremos que la suma está bien definida, es decir, que ese tercer punto existe y demostraremos que las curvas elípticas junto a esta operación de suma, es un grupo abeliano. El culmen de este trabajo es la demostración de la propiedad asociativa, algo que ocupará la mayor parte de este capítulo, para ser exactos toda la Sección 2.3. Antes de entrar de lleno en la demostración, la Subsección 2.3.1 se encargará de dejar claros los pasos que vamos a dar y el punto clave, el Teorema 2.3.2. De esta manera, el lector no debería perderse durante su desarrollo.

En el Capítulo 3 estudiaremos el Problema del Logaritmo Discreto, problema sobre el cual se basa la seguridad de las curvas elípticas en la criptografía. Formalmente y para cualquier grupo finito G, el Problema del logaritmo discreto es resolver una ecuación del tipo

$$a^x = b$$

con $x \in \mathbb{N}$ y $a, b \in G$.

En curvas elípticas, con notación aditiva, el problema equivale a dados dos puntos de la curva, encontrar el escalar por el cual se multiplicó uno para obtener el otro. No es un problema trivial siempre y cuando hagamos una buena elección del grupo de curvas elípticas. En este mismo capítulo veremos diferentes algoritmos existentes para intentar resolver este problema: Fuerza bruta, Index Calculus, Baby Step-Giant Step, algoritmos ρ y λ de Pollard y algoritmo de Pohlig-Hellman.

Por último, en el Capítulo 4 pasaremos a ver cómo se aplican las curvas elípticas a la criptografía. Los protocolos criptográficos de curva elíptica se basan en otros protocolos existentes de gran importancia, que será necesario estudiar antes. Veremos las operaciones criptográficas en general y como se resuelven en RSA, DH, DSA y AES. La última sección de este capítulo, la Sección 4.6, se dedica exclusivamente a estudiar las diferentes operaciones criptográficas utilizando curvas elípticas.

Abstract

The aim of the present work is to study the mathematical foundations on which the elliptical curves are based. Although new definitions are introduced, the majority of they derive from concepts seen in the subjects of Extension of Linear Algebra and Geometry, Groups and Rings and Algebraic Equations, then any student should be able to understand this document with relative facility. Nevertheless, since the algebra does not stop being abstract, to facilitate the understanding, we have tried to refresh all these concepts that can be a bit forgotten in our memory, before defining new others.

The study of the elliptical curves is not a really new topic. Elliptic curves have occupied a central paper in mathematics for three centuries and his notable arithmetical and geometric properties have found application in multiple problems and mathematical fields. Nevertheless, his employment in cryptography is recent, around the year 1985, thanks to Miller[3] and Koblitz[4].

Cryptography, from Greek kryptos, "hidden, secret" and graphos, "writing", is the practice and study of hiding information. It is the science used to transform the content of a message using a key, that is ciphering the message, so that if we send it through an insecure communication channel, nobody can decrypt it, only the recipient of the message.

There are evidences of the usage of cryptography 4000 years ago, in the egyptian town of Menet Khufu where the hieroglyphic inscriptions on the tomb of the nobleman KHNUMHOTEP II were written with unusual symbols to confuse or obscure the meaning of the inscriptions. Over time, with the arrival of machines, they replaced humans in the task of cipher messages. In 1916, it was patented in Netherlands one of the first cipher machines, the Arvid Gerhard Damm's machine, and in 1918, the famous machine ENIGMA. These machines were used exclusively to protect army's messages. However, just 40 years ago, this science has advanced a lot due to the introduction of computer system communications, and the rise of the Internet. Currentl cryptography is very present in our lifes, protecting each piece of information that we send through the net. Our money or the confidentiality of our personal data depends of the security of every process taking part in. The keystone for offering secure access and protected communications is the cryptography.

In a world where it is estimated that Google processes 25 petabytes of data everyday, Facebook shares more than 10 millions of photographys and every second, in Youtube, there is a new hour of video, cryptography has become essential. Email accounts, social networks, electronic transactions, all of them are protected by cryptosystems, that is, a set of algorithms that guarantee the information security. That is how cryptography, even without knowing it, is a daily reality.

Another field of the technology also grows: The Internet of the things (IoT). This concept comprises the union of the physical objects and the electronics, software, sensors and connectivity in order that it could achieve a major value and service across the exchange of information with the manufacturer, operator and other devices connected. Each of these objects is capable of interoperating in the current infrastructure of Internet. Nowadays, there already exist washers with WiFi; fridges that know the food that they contain and prepare for you the shopping list, lamps that they know when they have to turn on; "smart cities", where the illumination system is

[3] V. Miller: Use of elliptic curves in Cryptography, 1985
[4] N. Koblitz: Elliptic Curve Cryptography, 1987

efficient due to the information of many sensors, where the citizens use his mobile phone to interact with the services of the city, where the pollution is controlled... In a not very distant future, all the common objects of our house and city will be able to have connection to Internet, facilitating his management from the laptop, the tablet, the mobile phone or from a remote control center. Obviously, all these connections need to be protected (for example, we do not want that anybody with bad intentions turn on the lights while we are on vacation and, as a consequence, we receive an important receipt of electricity ...). These small devices are not conventional computers, that is, they do not have a great computacional power, a great RAM or a great hard disk.

In any case, the basis to guaranteeing secure access and protected communications is the cryptography, whose objetives are to ensure that the information is accessible only for an authorized person (**confidentiality**); that the message has not been manipulated (**integrity**); that the issuer has not been impersonated (**authenticity**); and that it is not possible that an issuer a message can deny that he sends it. Issuer and recipient have proofs that the receipt and the sending respectively has been carried out by the other part (**non-repudiation**).

Cryptography is typically divided into symmetric and asymmetric. The symmetric algorithms are characterized by the use of the same key to cipher and decipher. Both parts (issuer and receiver) must know the same key in advance. These algorithms are fast and use a key size of few bits (128, 256...). Unlike them, the asymmetric algorithms have two keys, the public key, that is available for anyone that wants to use it and the private key, that only his owner knows. In general, these algorithms are slower and need bigger keys (1024 bits, 2048 ...), but they are necessary to distribute a symmetric key to both entities in the communication or to do operations of digital signature [6] (authentication).

Additionally, it is expected that, with the proliferation of the concept of Internet-of-Things, a high number (hundreds of thousands) of constrained devices will need to exchange information safely. Due to his little computational resources, the symmetric cryptography might be a suitable alternative. Nevertheless, to assume the manual distribution of different symmetrical keys for every couple of devices becomes impossible in a context as Internet-of-Things. Therefore, asymmetric cryptography is necessary, since the only thing that the device needs to start working is his private/public key. However, the asymmetric current algorithms consume too many resources for a restricted device as in case of the Internet-of-Things networks.

Nowadays one of the more used algorithms is RSA. The problem is that there is an increasing need of bigger keys, since the calculation power of regular computers is increasing day by day, and a small key can be attacked easily. What will happen when the keys to cipher our information are so big that could not be processed in these small devices of restricted resources? The alternative is the use of elliptic curve algorithms. In those applications that need a high enough level of security, the cryptography of elliptical curves can provide this level destining fewer resources to obtain it. This means that in these limited devices, they can provide a very high security level very high without increasing the production cost of constrained devices. In particular, as we will see, the key size is smaller, and it implies fewer requirements of memory and offer faster cryptographic operations.

This work analyzes and studies the elliptical curve from a point of view of the mathematics that support this cryptographic scheme.

In order to know the mathematical base of this type of cryptography, we will need to start in Chapter 1 by remembering and extending our knowledge of finite fields $\mathbb{F}_q$ of order q, since elliptic curves are defined on them. Also we will revise the affine space and projective space in Section 1.2 because we are going to represent the points of the elliptic curve using the named homogeneous coordinates of the projective space, that will allow us to treat the points at the infinite as a common points. In this chapter we will see new concepts as singular points, flexes and the most important of all: intersection order. Intersection order can be defined both in the affine space and in the proyective space and in this chapter we will see that this concept is well defined, that is, it always exists. We will study a series of interesting properties that will allow

us to manipulate it better.

As soon as we have assimilated all the basic concepts, in Chapter 2 we will define what is an elliptic curve. We will see two ways of presenting. One way, more general, using Weierstrass's general equation,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

and other way, more simple, for bodies with characteristic different from two and three, using simplified equation of Weierstrass,

$$y^2 = x^3 + Ax + B,$$

where all the coefficients are in the field fixed for the elliptic curve.

In an elliptic curve, points can be added of the following way (Figure 3): If we have two points P, Q belonging to an elliptic curve, we can draw the line trough P and Q (if $P = Q$, it will be the tangent). This line will intersect the curve in the third point R. We will define $P + Q = -R$ as the symmetrical of R across the axis x.

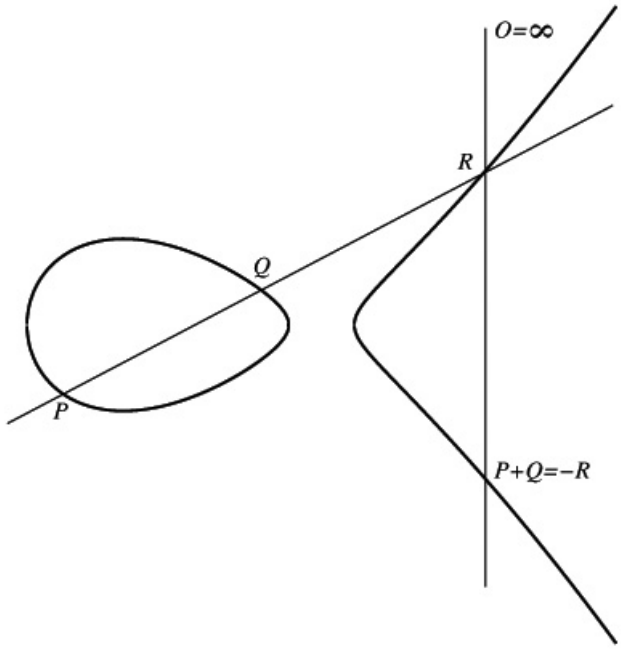

Figura 3: Adding points. **Source**: [7]

In Section 2.2, we will see that the sum is well defined, that is, that this third point exists and we will proof that elliptic curves with this operation, are an abelian group. The high point of this work is the proof of the associative property, something that will occupy most of this chapter, to be exact all Section 2.3. Before entering in the proof, Subsection 2.3.1 will introduce us in the proof in order that we have clear the steps that we are going to give and we have clear the key point, the Theorem 2.3.2, so that we do not get lost during his development.

In Chapter 3 we will study the Discreet Logarithm Problem, problem on which is based the safety of the elliptic curves cryptography. Formally and for any finite group G, the Discreet Logarithm Problem is to solve an equation of the type

$$a^x = b$$

with $x \in \mathbb{N}$ and $a, b \in G$.

It is not a trivial problem as long as we let's do a good choice of the elliptic curve group. In this same chapter we will see different existing algorithms to try to solve this problem: Brute force, Index Calculus, Baby Step-Giant Step, ρ and λ algorithms of Pollard and Pohlig-Hellman's algorithm.

Finally, in Chapter 4 we will see elliptic curves cryptography. The elliptic curves cryptographic protocols are based on other existing protocols of great importance, which will be necessary to study before. We will see the cryptographic operations in general and how they are solved in RSA, DH, DSA and AES. The last section of this chapter, Section 4.6, studies exclusively the different cryptographic operations using elliptic curves.

Introducción

La criptografía, de los términos griegos "krypt" (oculto) y "graphos" (escritura), es la ciencia de transformar el contenido de un mensaje mediante una clave, es decir cifrarlo, para que al ser emitido por un canal inseguro, no pueda ser descifrado más que por el destinatario.

Existen evidencias del uso de la criptografía durante la civilización egipcia hace nada menos que 4000 años donde se encontró sobre la tumba de un noble llamado Khnumhotep II un mesaje cifrado. Con el paso del tiempo y la llegada de las máquinas, éstas pasaron a relevar a los humanos de la ardua tarea de cifrar los mensajes. En 1916, se patentó en Holanda una de las primeras máquinas cifradoras, la máquina de Arvid Gerhard Damm y en 1918, la más famosa de todas: ENIGMA, creada por Arthur Scherbius. ENIGMA se lanzó inicialmente al mercado comercial, pero como la mayoría de este tipo de máquinas, acabó usándose para proteger mensajes del ejército. Sin embargo, desde hace apenas 40 años, esta ciencia avanza a pasos agigantados debido a la introducción de los sistemas informáticos en las comunicaciones y al auge de Internet. Actualmente está muy presente en nuestras vidas protegiendo cada trozo de información que mandamos por la red. Nuestro dinero o la confidencialidad de nuestros datos personales depende de que todos los procesos que intervienen sean suficientemente seguros.

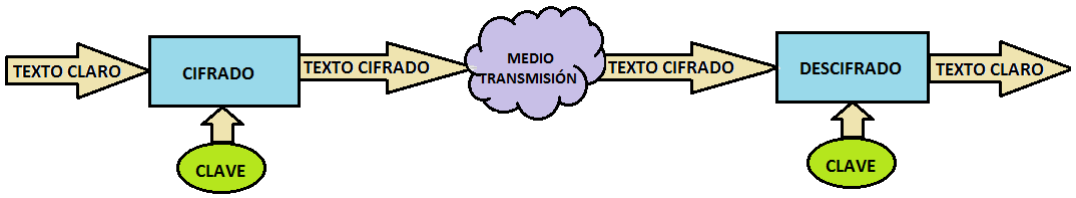

Figura 4: Proceso criptográfico

Los objetivos de la criptografía son garantizar que la información sea accesible únicamente por una persona autorizada (**confidencialidad**); que el mensaje no haya sido manipulado (**integridad**); que el emisor no haya sido suplantado (**autenticidad**); y que tanto emisor como receptor tengan pruebas de que la recepción y el envío respectivamente se ha llevado a cabo por la otra parte (**no repudio**).

En este trabajo analizaremos uno de los criptosistemas más prometedores de la actualidad: La curvas elípticas (ECC). Comenzaremos con unas nociones básicas de conceptos matemáticos que necesitaremos para situar las curvas elípticas en su espacio y poder entender los desarrollos posteriores. En el segundo capítulo entraremos de lleno en el tema, para definir lo que es una curva elíptica y demostraremos que forman un grupo abeliano prestando especial interés a la asociatividad, debido a su complejidad. Una vez que tenemos clara la base matemática sobre la que se sustentan las curvas elípticas, veremos el problema del logaritmo discreto. La dificultad de resolver este problema es lo que garantiza la seguridad no solo de este criptosistema, sino de otros muchos. Finalmente, veremos la aplicación de las curvas elípticas a la criptografía, entendiendo previamente las operaciones básicas criptográficas generales y los criptosistemas relacionados con ECC.

Estado del arte

Como dijimos al principio, la criptografía es una ciencia que va creciendo cada vez más. La información que transmitimos puede ser muy sensible como tarjetas de crédito y cuentas bancarias y necesitamos protegerla. Actualmente uno de los protocolos criptográficos que más se utilizan es RSA. El problema es que cada vez es se necesitan claves más grandes, ya que la potencia de cálculo de los ordenadores se va incrementando día a día, y una clave pequeña puede ser descifrada fácilmente[5].

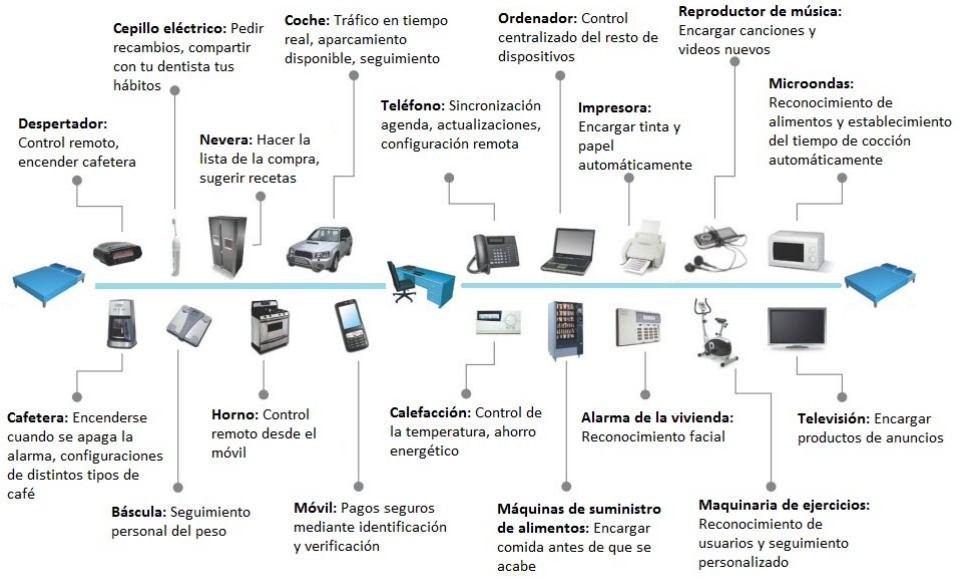

Figura 5: Internet de las cosas. **Fuente**: [23]

Otro campo de la tecnología también crece: El Internet de las cosas o Internet-of-Things (IoT). Este concepto supone la unión de los objetos físicos y la electrónica, software, sensores y conectividad a la red para que pueda lograr un mayor valor y servicio a través del intercambio de datos con el fabricante, operador y/u otros dispositivos conectados (Figura 5). Cada uno de esos objetos es capaz de interoperar en la infraestructura actual de Internet. Entre otros ejemplos, ya existen lavadoras con WiFi, neveras que saben los alimentos que contienen y preparan la lista de la compra, lámparas que saben cuando tienen que encenderse, ciudades inteligentes ("smart cities"), donde el alumbrado se lleva a cabo de forma eficiente mediante sensores, donde los ciudadanos utilizan su móvil para interactuar con los servicios de la ciudad, se controla la contaminación, etc. En un futuro no muy lejano todos los objetos comunes de nuestra casa y ciudad podrán disponer de conexión a Internet, facilitándonos su gestión a distancia desde el portátil, la tablet, el móvil o desde centro de control remotos. Obviamente, todas estas conexiones necesitan ser protegidas (por ejemplo, no queremos que alguien con malas intenciones encienda

[5]Existe una competición donde recompensan a las personas que logran factorizar números grandes, lo que implica romper RSA. Así se puede ir viendo qué tamaño de clave puede ser descifrada. `http://es.wikipedia.org/wiki/Competici%C3%B3n_de_factorizaci%C3%B3n_RSA`

las luces y la lavadora mientras estemos de vacaciones y nos venga una importante factura de la luz...). ¿Qué pasará cuando las claves de RSA sean tan grandes que no puedan ser procesadas en estos dispositivos? Una posible solución es el uso de protocolos criptográficos con curvas elípticas.

Lo bueno que tienen estos protocolos es que con una clave más pequeña, proporcionan la misma seguridad que RSA, lo que se traduce en menor memoria para almacenarlas y menor tiempo de cálculo. Perfecto para esos dispositivos.

El estudio de las curvas elípticas no es un tema realmente nuevo. Las curvas elípticas han ocupado un papel central en matemáticas desde hace tres siglos y sus notables propiedades aritméticas y geométricas han encontrado aplicación en múltiples problemas y campos matemáticos. Su empleo en criptografía es sin embargo reciente, pudiéndose situar su inicio en el año 1985, gracias a Miller[6] y Koblitz[7]. Actualmente, existen empresas que están realizando estudios de criptografía de curva elíptica en dispositivos de recursos limitados como la plataforma MBED. Este trabajo puede consultarse en [29].

La curvas elípticas también se utilizan en programas tan cotidianos como el Windows Media Player para proteger las claves de las licencias que autorizan a reproducir contenidos con DRM[33](Gestión digital de derechos) o en protocolos tan actuales como los bitcoins[22]. Los reproductores de Blu-Ray y la Play Station 3[27] implementan una tecnología similar para evitar la copia de contenidos mientras que la Wii[16] hace uso de las curvas elípticas para asegurar que nadie hace trampa cuando guardamos una partida on-line [12]. Los smartphones también utilizan curva elípticas para cifrar la información que transmiten. Incluso los nuevos pasaportes alemanes usan las curvas elípticas para proteger los datos biomédicos que almacenan. Aunque quizá el ejemplo más influyente de uso criptografía con curvas elípticas es la Suite B[21] del gobierno de los Estados Unidos. Dicha suite es un estándar federal de protección de documentos que actualmente usa algoritmos basados exclusivamente en curvas elípticas para cifrar documentos clasificados como críticos o confidenciales.

[6]V. Miller: Use of elliptic curves in Cryptography, 1985
[7]N. Koblitz: Elliptic Curve Cryptography, 1987

Capítulo 1

Nociones básicas

Comencemos introduciendo unas nociones básicas que serán fundamentales a la hora de seguir el texto.

A partir de ahora, K denotará un cuerpo, todos los espacios vectoriales serán espacios vectoriales sobre K, todos los polinomios tendrán coeficientes en K, lo que denotaremos como $f \in K[x]$ y trabajaremos sobre anillos conmutativos.

1.1. Cuerpos finitos

Antes de entrar de lleno en cuerpos finitos, necesitamos conocer una serie de defincciones y resultados sobre polinomios, anillos, grupos y dominios de integridad.

Definición 1.1.1. Sea un polinomio $f \in K[x]$ de grado m. Se dice que $a \in K$ es un **cero o una raíz de** f si $f(a) = 0$. Además, se dice que a es un cero f de **multiplicidad** $r \in \mathbb{Z}^+$ si $(x-a)^r | f$ y $(x-a)^{r+1} \nmid f$.

Definición 1.1.2. Una **extensión de cuerpos** es un par (K, F), donde F es un cuerpo y K es un subcuerpo. Lo denotaremos de la forma F/K y diremos que F es una extensión de K.

Definición 1.1.3. Sea K un cuerpo, $f \in K[x]$ con deg(f)= $r \geq 1$. Decimos que f se **escinde o factoriza** completamente sobre K cuando se verifica:

$$f = c(x - a_1)(x - a_2) \cdots (x - a_r)$$

con cada $x - a_i \in K[x]$.

Definición 1.1.4. Sea K un cuerpo, y sea P un conjunto de polinomios no constantes de $K[x]$. Una extensión F/K se llama **cuerpo de escisión** del conjunto P sobre K si todo $f \in P$ se escinde sobre F.

Proposición 1.1.5. *Sea K un cuerpo y sea P un conjunto de polinomios no constantes de K[x]. Existe un cuerpo de escisión de P sobre K y es único salvo K-isomorfismos.*

Demostración. Puede encontrarse en [26]. □

Definición 1.1.6. Un grupo se llama finito cuando tiene un número finito de elementos. El número de elementos de un grupo se llama su **orden**. Si un grupo no es finito, se dice también que tiene orden infinito. El orden de un grupo G se suele denotar $|G|$.

Definición 1.1.7. Sea G un grupo y sea C un subconjunto suyo. El menor subgrupo de G que contiene a C se denomina **subgrupo generado por C** y se denota $\langle C \rangle$. Si $\langle C \rangle = G$, se dice que C es un conjunto generador de G.

Definición 1.1.8. Un grupo G es cíclico si existe un elemento $g \in G$ tal que $\langle g \rangle = G$. En tal caso, se dice que g es un **generador** de G.

Definición 1.1.9. Sea A un anillo. Si $a, b \in A$ cumplen que $ab = 1$, entonces decimos que a y b son **unidades** del anillo A. El conjunto $U(A)$ de todas las unidades de A es un grupo abeliano $(U(A), \cdot)$, donde $\cdot$ es la multiplicación en A restringida a $U(A)$. $U(A)$ también suele escribirse como A^*. En el caso de $\mathbb{Z}_n$, se denota $\mathbb{Z}_n^*$

Definición 1.1.10. Un **cuerpo** es un anillo conmutativo $(A, +, \cdot)$ donde $1 \neq 0$ y para todo elemento no nulo $a \in A$, existe un elemento $c \in A$ de forma que $ac = 1$, es decir si todo elemento no nulo tiene inverso. Si el cuerpo $\mathbb{F}$ es finito de orden q, lo denotaremos $\mathbb{F}_q$.

Proposición 1.1.11. *Sea K un cuerpo, y sea G un subgrupo del grupo formado por todos los elementos no nulos de K con la multiplicación. Si G es finito, entonces G es cíclico.*

Demostración. Sea $|G| = n$. Como G es abeliano, es isomorfo a un producto de grupos cíclicos en la forma

$$G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_s},$$

donde los d_i son enteros positivos tales que $d_1|d_2|...|d_s$.

Notemos que el orden de G es igual al del producto anterior, por tanto $n = d_1 d_2 ... d_s$. Se tiene que $s \geq 1$, y G es cíclico si $s = 1$. Queremos ver por tanto, que $s = 1$.

Usamos ahora notación multiplicativa para los $\mathbb{Z}_{d_i}$, es decir, identificamos $\mathbb{Z}_{d_i} = C_{d_i}$, siendo C_{d_i} el grupo cíclico multiplicativo de orden d_i. Cada elemento g de cada uno de los factores $C_{d_i} \cong \mathbb{Z}_{d_i}$ verifica que $g^{d_i} = 1 = g^{d_s}$, ya que $d_i|d_s$. Por tanto, todo elemento $a = (a_1, ..., a_s)$ del grupo producto dado arriba (isomorfo a G), verifica $a^{d_s} = (1, ..., 1) = 1$. En virtud del isomorfismo, tendremos que $b^{d_s} = 1$ para todo $b \in G$.

Esto quiere decir que todo elemento $G \subseteq K$ es solución de la ecuación $x^{d_s} - 1 = 0$. Por tanto el polinomio $x^{d_s} - 1$ tiene al menos n raíces distintas en K. En consecuencia, su grado d_s ha de cumplir $d_s \geq n$. Como n es el producto de los d_i, debe tenerse $d_s = n$ y $s = 1$, como queríamos ver. □

Corolario 1.1.12. *Sea F un cuerpo finito de q elementos. El grupo multiplicativo $\mathbb{F}^*$ de las unidades de F es un grupo cíclico de $q - 1$ elementos.*

Definición 1.1.13. Diremos que un cuerpo K (o un anillo) tiene **característica** n si n es el menor número natural tal que $1 + 1 + ...^n ... + 1 = 0$, es decir, si $n1_A = 0$ para todo $a \in A$. Si esta suma nunca se anulase, se dice que el cuerpo tiene característica cero. La notación habitual es $char(K) = n$.

Definición 1.1.14. Sea A un anillo. Un elemento $a \in A$ se dice que es **regular** si se verifica que para todo $x \in A$, si $ax = 0$ necesariamente $x = 0$. En caso contrario se dice que es un **divisor de cero**.

Definición 1.1.15. Un **dominio de integridad** es un anillo donde $1 \neq 0$ y no existen divisores de cero.

Proposición 1.1.16. *Sea A un anillo conmutativo y sea I un ideal propio de A. Entonces I es un ideal primo si y sólo si el anillo cociente A/I es un dominio.*

Demostración. Sea I primo. Sea $a + I \in A/I$ un elemento no nulo. Entonces $a \notin I$. Supongamos ahora que $(a + I)(b + I) = 0 = I$, de modo que tendremos $ab + I = 0 = I$ y $ab \in I$. Por hipótesis, será $b \in I$, y por tanto $b + I = 0$. Esto muestra que cada elemento no nulo de A/I no es divisor de cero.

Recíprocamente, supongamos que A/I es un dominio, y sea $ab \in I$ con $a \notin I$, $b \in A$. Entonces $a + I \neq 0$ y $(a + I)(b + I) = ab + I = 0$. Por la hipótesis $b + I = 0 = I$ y así $b \in I$. Luego I es un ideal primo. □

Observación. Como cualquier anillo A cumple que $A \cong A/(0)$, se tiene que A es un dominio si y sólo si el ideal trivial (0) es primo.

Para los anillos $\mathbb{Z}_n$ deducimos que $\mathbb{Z}_n$ es un dominio si y sólo si n es un número primo. Cuando n no es primo, el anillo $\mathbb{Z}_n$ tiene divisores de cero.

Proposición 1.1.17. *La característica de un dominio de integridad A es 0 o un número primo.*

Demostración. Consideremos la aplicación $\phi : \mathbb{Z} \to A$ dada por $n \to n1_A$. Esta aplicación ϕ es un homomorfismo de anillos. En efecto,

$$\phi(a+b) = (a+b)1 = a1 + b1 = \phi(a) + \phi(b),$$

$$\phi(ab) = ab1 = (a1)(b1) = \phi(a)\phi(b),$$

$$\phi(1) = 1.$$

Además $Ker(\phi) = \{n \in \mathbb{Z} : n1_A = 0\}$ y es un subanillo de $\mathbb{Z}$. Por tanto, puede ocurrir:

1. $Ker(\phi) = (0)$. Entonces ϕ es inyectiva y el orden aditivo de 1 es infinito. Se tiene que $char(A) = 0$.
2. $Ker(\phi) = \mathbb{Z}$. En este caso $A = 0$ y esto no es posible si $1 \neq 0$ en el anillo A
3. $Ker(\phi) = n\mathbb{Z}$ con $n \neq 0, 1$. Entonces n es el orden aditivo de 1 y $char(A) = n$.

En resumen, el núcleo de ϕ es el ideal de $\mathbb{Z}$ generado por la característica de A. Por el Primer Teorema de Isomorfía, tenemos que si $char(A) = n$, entonces A tiene un subanillo isomorfo a $\mathbb{Z}_n$. Como A es un dominio se tiene que $\mathbb{Z}_n$ también lo es, y por la observación anterior, $n = 0$ ó n es primo. □

Teorema 1.1.18. *1. Si F es un cuerpo finito entonces el cardinal de F es una potencia de un primo y este primo es su característica.*

2. Para cada cada potencia de un primo q, existe un cuerpo con q elementos. Los elementos de dicho cuerpo son los ceros del polinomio $x^q - x$ en un cuerpo algebraicamente cerrado.

3. Dos cuerpos finitos con el mismo cardinal son isomorfos

4. Si F es un cuerpo con q elementos y F′ es un cuerpo con q′ elementos, entonces F′ contiene un subcuerpo isomorfo a F si y sólo si q′ es potencia de q.

Demostración. 1. Por la Proposición 1.1.17, si F es un cuerpo finito, entonces $char(F)$ es 0 o un número primo. Además, si $p = Char(F)$, entonces F contiene al cuerpo $\mathbb{Z}_p$ y F tiene una estructura de espacio vectorial sobre $\mathbb{Z}_p$. Si este espacio vectorial tiene dimensión n, entonces F es isomorfo a $\mathbb{Z}_p^n$ como espacio vectorial, y entonces F tiene p^n elementos.

2. Fijamos un cuerpo F algebraicamente cerrado con $char(F) = p$ y para cada $n \geq 0$ consideramos el conjunto

$$F_{p^n} = \{a \in F : a^{p^n} = a\}. \tag{1.1}$$

Se tiene que F_{p^n} son los ceros del polinomio $f = x^{p^n} - x$. Este polinomio no tiene ceros múltiples ya que $f = x(x^{p^n-1} - 1) = xg$ y el único cero de $g' = (p^n - 1)x^{p^n-2}$ no es cero de g. Esto significa que F_{p^n} tiene exactamente p^n elementos. Vamos a ver que es subcuerpo de F, y por tanto cuerpo:

- $0, 1 \in F_{p^n}$,
- si $a, b \in F_{p^n}$, entonces $-a, ab \in F_{p^n}$,
- si $0 \neq a \in F_{p^n}$ entonces $a^{-1} \in F_{p^n}$,
- si $a, b \in F_{p^n}$, entonces $a + b \in F_{p^n}$. Esta propiedad se tiene por el hecho de que si $0 < i < p$, entonces p divide a $\binom{p}{i} = \frac{p!}{i!(p-i)!}$, y por tanto

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i = a^p + b^p.$$

Por inducción en n se ve fácilmente que $(a+b)^{p^n} = a^{p^n} + b^{p^n} = a+b$, luego $a, b \in F_{p^n}$.

De esta manera, F_{p^n} es un cuerpo con p^n elementos. En particular, dentro de cada cuerpo algebraicamente cerrado F con $char(F) = p$, existe un cuerpo con n elementos, que es lo que queríamos demostrar.

3. Esto equivale a probar la unicidad del apartado anterior salvo isomorfismos. Si K es un subcuerpo de F con p^n elementos entonces K^* es un grupo de orden $p^n - 1$, y por tanto todos lo elementos no nulos de K^* son ceros del polinomio $x^{p^n-1} - 1$ y todos los elementos de K son ceros de $f = x^{p^n} - x = x(x^{p^n-1} - 1)$. O sea, $K = F_{p^n}$. De esta manera, el único subcuerpo de F con p^n elementos es exactamente F_{p^n}, formado por los ceros del polinomio f en F. Podemos observar que además, es el cuerpo de escisión de f sobre $\mathbb{Z}_p$. Aplicando la Proposición 1.1.5, tenemos que todos los cuerpos de la forma F_{p^n} con F algebraicamente cerrado son isomorfos.

4. $\Leftarrow$: Sean $q' = p^{nm}$ y $q = p^n$. Como los ceros de $x^{p^n} - x$ son también ceros de $x^{p^{nm}} - x$ para todo m, se tiene que $F_{p^n} \subseteq F_{p^{nm}}$, que es lo que queríamos.
$\Rightarrow$: Llamemos $q' = p^k$ y $q = p^n$. Si $F_{p^n} \subseteq F_{p^k}$, entonces F_{p^k} es un espacio vectorial de dimensión finita sobre F_{p^n}, con lo que $p^k = |F_{p^k}|$ es una potencia de $p^n = |F_{p^n}|$ (es decir, k es múltiplo de n).

□

Notación. Si E/F es una extensión de cuerpos y $\alpha \in E$, entonces $F[\alpha]$ denota el menor subcuerpo de E que contiene a F y a α.

Proposición 1.1.19. *Sea $F = K$ una extensión de cuerpos algebraica, sea $f \in K[x]$ un polinomio no constante y sea $\alpha \in F$ un elemento arbitrario. Diremos que:*

1. *El polinomio f es separable si f no tiene raíces múltiples en una clausura algebraica de K.*
2. *El elemento α es separable sobre K si $Irr(\alpha, K)$ es un polinomio separable, donde $Irr(\alpha, K)$ denota el polinomio irreducible de α sobre K.*
3. *La extensión $F = K$ es separable si todo $\alpha \in F$ es un elemento separable sobre K.*

Teorema 1.1.20 (Teorema del elemento primitivo)**.** *Si F/K es una extensión finita y separable, entonces F/K es simple, es decir, existe $\alpha \in F$ tal que $F = K[\alpha]$.*

Demostración. Puede encontrarse en [26]. □

Para construir un cuerpo finito con $q = p^n$ elementos para un p primo y un entero positivo n, usamos la siguiente proposición:

Proposición 1.1.21. *Para todo $n \geq 1$ existe un polinomio irreducible f de grado n sobre F_p. En tal caso $F[x]/(f)$ es un cuerpo con q elementos.*

Demostración. Sea la extensión E/F y sea $\alpha \in E$ algebraico sobre F. Entonces la aplicación

$$S_\alpha : F[x] \longrightarrow E$$

$$f \longrightarrow f(\alpha)$$

no es inyectiva. Como E es un cuerpo, el núcleo P de S_α es un ideal de $F[x]$ y $P = (Irr(\alpha, F))$, donde $Irr(\alpha, F)$ es el polinomio irreducible mónico de $F[x]$ que tiene a α como cero. La dimensión de $F[\alpha]$ sobre F es el grado de este polinomio.
Así, si $q = p^n$ con n primo, por el Teorema 1.1.20 se tiene que $F_q = F_p[\alpha]$ para algún $\alpha \in F_q$ y como F_q tiene dimensión n sobre F, el polinomio $Irr(\alpha, F_p)$ tiene grado n, pues por el Primer Teorema de Isomorfía, $F_q \simeq F_p[x]/p$. □

1.2. El espacio afín y el espacio proyectivo

En esta parte se pretende dar una pequeña introducción al espacio proyectivo sobre un cuerpo K, $\mathbb{P}^2(K)$, ya que es el mundo donde "viven"las curvas elípticas. Además, muchos de los conceptos que se van a manejar utilizan el espacio proyectivo. Este espacio, a diferencia del espacio afín, nos va a permitir tratar al infinito como un punto más, algo que nos facilitará mucho las cosas a la hora de trabajar en una curva elíptica.

1.2.1. El espacio afín

Definición 1.2.1. Un **espacio afín** es una terna $(\mathbb{A}, V, \phi)$ formada por un conjunto $\mathbb{A}$, un espacio vectorial V sobre un cuerpo K y una aplicación $\phi : \mathbb{A} \times V \longrightarrow \mathbb{A}$, que denotaremos $\phi(P, v) := P + v$, para todo $P \in \mathbb{A}$ y $v \in V$ que cumple que para todo $P, Q \in \mathbb{A}$ y para todo $v, w \in V$:

1. $P + (v + w) = (P + v) + w$,
2. $P + 0 = P$,
3. y existe un único $u \in V$ tal que $P + u = Q$.

Observación. Sea V un espacio vectorial sobre un cuerpo K. La aplicación $\phi : V \times V \longrightarrow V$, dada por $\phi(v, w) = v + w$ induce en V una estructura natural de espacio afín. Un caso particular es K^n con $n \in \mathbb{N}$. Este espacio se suele denotar $\mathbb{A}^n(K)$.

Definición 1.2.2. Una recta en el plano afín $\mathbb{A}^2(K)$, que pasa por $P \in \mathbb{A}^2(K)$ con la dirección de $0 \neq v \in V$ es el conjunto

$$P + < v >= \{P + \lambda v\}_{\lambda \in K}.$$

Definición 1.2.3. Una recta se dice que es **vertical** si está dada por la ecuación $x = x_0$, con x_0 constante.

Definición 1.2.4. Dado $P \in K[x, y] \setminus \{0\}$, se define una **curva algebraica** en $\mathbb{A}^2(K)$ como el conjunto de puntos $x \in \mathbb{A}^2(K)$ que satisfacen $P(x) = 0$.

Definición 1.2.5. Una curva dada por la ecuación $F(x, y, z) = 0$ se dice **irreducible** si F es un polinomio irreducible.

Definición 1.2.6. Un **cambio de coordenadas en** $\mathbb{A}^2(K)$ es una aplicación

$$\varphi : K^2 = \mathbb{A}^2(K) \to \mathbb{A}^2(K) = K^2$$

dada por $\varphi(x) = Ax + b$, donde $A \in GL_2(K)$ y $b \in K^2$.

1.2.2. El espacio proyectivo

Consideremos la relación de equivalencia en $K^{n+1} \setminus \{0\}$:

$$P \sim Q \text{ si y sólo si existe } \lambda \neq 0 \text{ tal que } Q = \lambda P.$$

Definición 1.2.7. Al conjunto cociente de esa relación de equivalencia lo llamaremos **espacio proyectivo** $\mathbb{P}^n(K) = \dfrac{K^{n+1} \setminus \{0\}}{\sim}$.

Notación. Si $P = (x_1, ...x_n)$, denotaremos a su clase de equivalencia en el espacio proyectivo $[x_1, ..., x_n]$.

De esta manera los puntos del espacio proyectivo son en realidad rectas vectoriales que pasan por el origen.

Si $P = (x_1, ...x_n)$ y $x_n \neq 0$, tenemos que $[x_1, ..., x_n] = \left[\dfrac{x_1}{x_n}, ..., \dfrac{x_{n-1}}{x_n}, 1\right]$. En el caso $x_n = 0$ se denominan puntos del infinito, $[x_1, ..., x_{n-1}, 0]$.
Además, tenemos la inclusión del espacio afín en el plano proyectivo

$$\mathbb{A}^n(K) \hookrightarrow \mathbb{P}^n(K)$$

$$(x_1, ...x_n) \rightsquigarrow [x_1, ..., x_{n-1}, 1]$$

lo que significa que $\mathbb{P}^n(K)$ se puede identificar con los puntos de $\mathbb{A}^n(K)$ junto con los puntos del infinito.

Veamos que ocurre con los polinomios cuando estamos en el espacio proyectivo. Nos van a interesar especialmente este tipo de polinomios:

Definición 1.2.8. Un polinomio se dice que es **homogéneo** cuando es suma de monomios del mismo grado.

Así, podemos **homogeneizar** un polinomio $f(x_1, ..., x_n)$ añadiéndole una tercera variable x_{n+1} que complete los grados de los monomios, por ejemplo si $f(x, y) = y^2 - x^3 - ax - b$ entonces el homogeneizado de f es $F(x, y, z) = y^2z - x^3 - axz^2 - bz^3$.

De la misma manera, podemos **deshomogeneizar** un polinomio homogéneo evaluando en el uno la variable extra que hemos añadido, volviendo al polinomio original. Así obtenemos la siguiente proposición:

Proposición 1.2.9. *Sea $f(x_1, ...x_{n-1})$ un polinomio de grado m, y sea $F(x_1, ...x_n)$ el polinomio f homogeneizado. Entonces se cumple:*

$$f(x_1, ...x_{n-1}) = F(x_1, ...x_{n-1}, 1),$$

$$F(x_1, ...x_n) = x_n^m f\left(\frac{x_1}{x_n}, ..., \frac{x_{n-1}}{x_n}\right).$$

Una vez claros estos conceptos, podemos centrarnos en lo que ocurre en el espacio proyectivo.

Proposición 1.2.10. *Sean $(x, y, z) \sim (u, v, w)$ y F un polinomio homogéneo. Entonces $F(x, y, z) = 0$ si y solo si $F(u, v, w) = 0$.*

Demostración. Si $(x_1, ..., x_n) \sim (u_1, ..., u_n)$, entonces existe un escalar no nulo λ tal que $u_1 = \lambda x_1$,..., $u_n = \lambda x_n$. Como $F(\lambda x_1, ..., \lambda x_n) = \lambda^{gradoF} F(x_1, ...x_n) = 0$ se tiene que $F(x_1, ...x_n) = 0$ y por tanto $F(\lambda x_1, ..., \lambda x_n) = 0$.

□

Esta proposición nos da un resultado importante: Los ceros de un polinomio homogéneo F no dependen del representante elegido; los ceros de F en $\mathbb{P}^2(K)$ están bien definidos. Si el polinomio no es homogéneo esto no tiene por qué ocurrir, por lo que nos interesará trabajar solo con homogéneos.

Definición 1.2.11. Una recta en el plano proyectivo $\mathbb{P}^2(K)$ es el conjunto de puntos $[x, y, z] \in \mathbb{P}^2(K)$ que satisfacen una ecuación $ax + by + cz$ para un $(a, b, c) \in K^3 \setminus (0, 0, 0)$.

Obsérvese que los puntos $(x, y, z) \in K^3$ para los que $[x, y, z]$ está en la recta de ecuación $ax+by+cz = 0$ forman un subespacio vectorial V de dimensión 2 de K^3. Por tanto, estos puntos pueden ser dados por ecuaciones paramétricas:

$$\begin{cases} x = a_1u + b_1v \\ y = a_2u + b_2v \\ z = a_3u + b_3v \end{cases} \tag{1.2}$$

donde $u, v \in K$ y $(u, v) \neq (0, 0)$, de forma que $(a_1, a_2, a_3), (b_1, b_2, b_3)$ es una base de V, o matricialmente:

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \\ a_3 & b_3 \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}. \tag{1.3}$$

Con lo que la recta está formada por los puntos con coordenadas homogéneas $[x, y, z]$ que se pueden expresar como en (1.2) (equivalentemente (1.3)) con $(u, v) \in \mathbb{P}^1(K)$.

Si todos los pares (a_i, b_i) fuesen múltiplos, $(a_i, b_i) = \lambda_i(a_j, b_j)$, entonces $(x, y, z) = x(1, \lambda_2, \lambda_3)$, luego en el espacio proyectivo no tendríamos una recta, sino un punto. Para asegurar que (1.3) efectivamente representa una recta en el espacio proyectivo, utilizamos la siguiente proposición, cuya demostración es evidente por lo que acabamos de explicar.

Proposición 1.2.12. *Sea*

$$M = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \\ a_3 & b_3 \end{pmatrix}. \tag{1.4}$$

Entonces Rang$(M) = 2$, donde Rang(M) denota el rango de la matriz M, si y solo si los elementos $[x, y, x] \in \mathbb{P}^2(K)$ con (x, y, x) de la forma (1.3) para algún $(u, v) \in K^2 \setminus \{0\}$, forman una recta del plano proyectivo $\mathbb{P}^2(K)$.

Definición 1.2.13. Dado $P \in K[x, y, z] \setminus \{(0, 0, 0)\}$ un polinomio homogéneo, se define una **curva proyectiva** de $\mathbb{P}^2(K)$ como el conjunto de puntos $x \in \mathbb{P}^2(K)$ que satisfacen $P(x) = 0$.

Definición 1.2.14. Un **cambio de coordenadas en** $\mathbb{P}^2(K)$ es una aplicación

$$\varphi : \mathbb{P}^2(K) \to \mathbb{P}^2(K)$$

dada en coordenadas homogéneas por $\varphi(x) = Ax$, donde $A \in GL_3(K)$.

Proposición 1.2.15. *Dados $P_1, P_2, P_3, P_4 \in \mathbb{P}^2(K)$, tres de ellos no alineados, existe un único cambio de coordenadas φ tal que $\varphi(P_1) = [1, 0, 0]$, $\varphi(P_2) = [0, 1, 0]$, $\varphi(P_3) = [0, 0, 1]$ y $\varphi(P_4) = [1, 1, 1]$.*

Demostración. Podemos escribir el cambio de coordenadas como un producto de matrices:

$$\begin{pmatrix} \alpha_{0,0} & \alpha_{0,1} & \alpha_{0,2} \\ \alpha_{1,0} & \alpha_{1,1} & \alpha_{1,2} \\ \alpha_{2,0} & \alpha_{2,1} & \alpha_{2,2} \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_0' \\ x_1' \\ x_2' \end{pmatrix}. \tag{1.5}$$

Sea $P_i = [a_{i,0}, a_{i,1}, a_{i,2}]$ con $i = 1, 2, 3, 4$. Nuestro objetivo es encontrar una matriz $\{\alpha_{i,j}\}$ con determinante no nulo, tal que las siguientes condiciones se satisfagan con una elección adecuada de $r, s, t, u \neq 0$:

$$\begin{pmatrix} \alpha_{0,0} & \alpha_{0,1} & \alpha_{0,2} \\ \alpha_{1,0} & \alpha_{1,1} & \alpha_{1,2} \\ \alpha_{2,0} & \alpha_{2,1} & \alpha_{2,2} \end{pmatrix} \begin{pmatrix} a_{1,0} \\ a_{1,1} \\ a_{1,2} \end{pmatrix} = \begin{pmatrix} r \\ 0 \\ 0 \end{pmatrix}, \tag{1.6}$$

$$\begin{pmatrix} \alpha_{0,0} & \alpha_{0,1} & \alpha_{0,2} \\ \alpha_{1,0} & \alpha_{1,1} & \alpha_{1,2} \\ \alpha_{2,0} & \alpha_{2,1} & \alpha_{2,2} \end{pmatrix} \begin{pmatrix} a_{2,0} \\ a_{2,1} \\ a_{2,2} \end{pmatrix} = \begin{pmatrix} 0 \\ s \\ 0 \end{pmatrix}, \tag{1.7}$$

$$\begin{pmatrix} \alpha_{0,0} & \alpha_{0,1} & \alpha_{0,2} \\ \alpha_{1,0} & \alpha_{1,1} & \alpha_{1,2} \\ \alpha_{2,0} & \alpha_{2,1} & \alpha_{2,2} \end{pmatrix} \begin{pmatrix} a_{3,0} \\ a_{3,1} \\ a_{3,2} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ t \end{pmatrix}, \tag{1.8}$$

$$\begin{pmatrix} \alpha_{0,0} & \alpha_{0,1} & \alpha_{0,2} \\ \alpha_{1,0} & \alpha_{1,1} & \alpha_{1,2} \\ \alpha_{2,0} & \alpha_{2,1} & \alpha_{2,2} \end{pmatrix} \begin{pmatrix} a_{4,0} \\ a_{4,1} \\ a_{4,2} \end{pmatrix} = \begin{pmatrix} u \\ u \\ u \end{pmatrix}. \tag{1.9}$$

Despejando las matrices a la derecha de la igualdad (la matriz $\{\alpha_{i,j}\}$ tiene inversa porque los puntos no están alineados) y posteriormente multiplicando por los inversos de r, s, t, u, nos queda que las condiciones anteriores son equivalentes a :

$$\begin{pmatrix} \beta_{0,0} & \beta_{0,1} & \beta_{0,2} \\ \beta_{1,0} & \beta_{1,1} & \beta_{1,2} \\ \beta_{2,0} & \beta_{2,1} & \beta_{2,2} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} ra_{1,0} \\ ra_{1,1} \\ ra_{1,2} \end{pmatrix}, \tag{1.10}$$

$$\begin{pmatrix} \beta_{0,0} & \beta_{0,1} & \beta_{0,2} \\ \beta_{1,0} & \beta_{1,1} & \beta_{1,2} \\ \beta_{2,0} & \beta_{2,1} & \beta_{2,2} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} sa_{2,0} \\ sa_{2,1} \\ sa_{2,2} \end{pmatrix}, \tag{1.11}$$

$$\begin{pmatrix} \beta_{0,0} & \beta_{0,1} & \beta_{0,2} \\ \beta_{1,0} & \beta_{1,1} & \beta_{1,2} \\ \beta_{2,0} & \beta_{2,1} & \beta_{2,2} \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} ta_{3,0} \\ ta_{3,1} \\ ta_{3,2} \end{pmatrix}. \tag{1.12}$$

Claramente, las tres primeras condiciones se satisfacen para todo r, s, t haciendo

$$\begin{pmatrix} \beta_{0,0} & \beta_{0,1} & \beta_{0,2} \\ \beta_{1,0} & \beta_{1,1} & \beta_{1,2} \\ \beta_{2,0} & \beta_{2,1} & \beta_{2,2} \end{pmatrix} = \begin{pmatrix} r\alpha_{1,0} & s\alpha_{2,0} & t\alpha_{3,0} \\ r\alpha_{1,1} & s\alpha_{2,1} & t\alpha_{3,1} \\ r\alpha_{1,2} & s\alpha_{2,2} & t\alpha_{3,2} \end{pmatrix}. \tag{1.13}$$

Para que se se satisfaga la última condición, basta determinar $r.s.t$ tal que

$$\begin{pmatrix} r\alpha_{1,0} & s\alpha_{2,0} & t\alpha_{3,0} \\ r\alpha_{1,1} & s\alpha_{2,1} & t\alpha_{3,1} \\ r\alpha_{1,2} & s\alpha_{2,2} & t\alpha_{3,2} \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} a_{4,0} \\ a_{4,1} \\ a_{4,2} \end{pmatrix}, \tag{1.14}$$

que es equivalente al sistema de ecuaciones

$$\begin{pmatrix} \alpha_{1,0} & \alpha_{2,0} & \alpha_{3,0} \\ \alpha_{1,1} & \alpha_{2,1} & \alpha_{3,1} \\ \alpha_{1,2} & \alpha_{2,2} & \alpha_{3,2} \end{pmatrix} \begin{pmatrix} r \\ s \\ t \end{pmatrix} = \begin{pmatrix} a_{4,0} \\ a_{4,1} \\ a_{4,2} \end{pmatrix}. \tag{1.15}$$

Tenemos un sistema de ecuaciones con tres ecuaciones y tres incógnitas, cuyo determinante es no nulo, ya que los puntos P_1, P_2, P_3 no están alineados. Por la regla de Cramer, este sistema tiene una solución única (r_0, s_0, t_0), lo que completa la prueba. □

Proposición 1.2.16. *Dados $P_1, P_2, P_3, P_4 \in \mathbb{P}^2(K)$, tres de ellos no alineados, y $Q_1, Q_2, Q_3, Q_4 \in \mathbb{P}^2(K)$ cumpliendo lo mismo, existe un único cambio de coordenadas φ tal que $\varphi(P_i) = Q_i$ para $i = 1, 2, 3$.*

Demostración. Por la Proposición 1.2.15, existe un cambio de coordenadas ψ que lleva P_1 a $[1, 0, 0]$, P_2 a $[0, 1, 0]$, P_3 a $[0, 0, 1]$ y P_4 a $[1, 1, 1]$.

Por la misma proposición, existe otro cambio de coordenadas γ que lleva Q_1 a $[1, 0, 0]$, Q_2 a $[0, 1, 0]$, Q_3 a $[0, 0, 1]$ yQ_4 a $[1, 1, 1]$.

Tomando $\varphi = \gamma^{-1} \circ \psi$, tenemos lo que queremos. □

Si C es la curva determinada por el polinomio F y φ es un cambio de coordenadas, denotaremos $F^{\varphi} = F \circ \varphi^{-1}$.

Observación. Si tenemos una curva proyectiva $F(K) \in K[x, y, x]$, y tomamos $P \in F(K)$, podemos elegir φ cambio de coordenadas que nos lleve P a donde queramos, por ejemplo $\varphi(P) = (0, 0) = [0, 0, 1]$.

Definición 1.2.17. El **grado** de una curva del plano afín o proyectivo es el grado del polinomio que la representa. En el caso en el que una curva pueda representarse mediante varios polinomios, por ejemplo x, x^2, se tomará el de menor grado.

Definición 1.2.18. Dos curvas C_1 y C_2 se dice que son **equivalentes** si existe un cambio de coordenadas afines ϕ (coordenadas homogéneas en el caso de curvas proyectivas) tal que $P \in C_1$ si y sólo si $P \in C_2$.

1.2.3. Orden de intersección

A partir de ahora, dada una parametrización $H(t)$ de una curva o recta, diremos que un punto (x, y) corresponde a $t = t_0$ si $H(t_0) = (x, y)$.

Definición 1.2.19. Sea $f(x, y)$ un polinomio que describe una curva C en el plano afín, y sea una recta L con ecuaciones paramétricas en función del parámetro t:

$$x = a_1 t + b_1, \qquad y = a_2 t + b_2. \tag{1.16}$$

Sea $\widetilde{f}(t) = f(a_1 t + b_1, a_2 t + b_2)$. Decimos que **L intersecta a C con orden n** en el punto (x,y) correspondiente a $t = t_0$ si $(t - t_0)^n$ es la mayor potencia de $(t - t_0)$ que divide a $\widetilde{f}(t)$.

Observación. Utilizando un cambio de coordenadas, podemos tomar $t_0 = 0$, y entonces el orden de intersección sería la multiplicidad del cero como raíz (es decir, como cero) de $\widetilde{f}(t)$.

Definición 1.2.20 (**Versión homogénea**)**.** Sea $F(x,y,z)$ un polinomio homogéneo y sea C la curva en el espacio proyectivo descrita por $F=0$. Sea una recta L con ecuaciones paramétricas en función de (u,v):

$$x = a_1u + b_1v, \qquad y = a_2u + b_2v, \qquad z = a_3u + b_3v. \tag{1.17}$$

Sea $\widetilde{F}(u,v) = f(a_1u+b_1v, a_2u+b_2v, a_3u+b_3v)$. Decimos que **L intersecta a C con orden n** en el punto $P=[x_0,y_0,z_0]$ correspondiente a $[u,v]=[u_0,v_0]$ si $(v_0u-u_0v)^n$ es la mayor potencia de (v_0u-u_0v) que divide a $\widetilde{F}(u,v)$. Vamos a denotarlo $ord_{L,P}(F)=n$.

Nota. Por convenio, si $\widetilde{F}=0$, es decir $L\subseteq C$, se toma $ord_{L,P}(F)=\infty$.

Observación. Si en el caso homogéneo tomamos $v=v_0=1$ obtenemos el caso no homogéneo, luego ambas formulaciones son equivalentes. Sin embargo, como dijimos anteriormente, nos interesa más trabajar en el espacio proyectivo ya que tiene la ventaja de tratar a los puntos del infinito como al resto de puntos.

La siguiente proposición nos garantiza la existencia del orden.

Proposición 1.2.21. *Sea $G(u,v)$ un polinomio homogéneo no nulo y sea $[u_0,v_0]\in\mathbb{P}^1(K)$. Entonces existe un entero $k\geq 0$ y un polinomio $H(u,v)$ con $H(u_0,v_0)\neq 0$ tal que*

$$G(u,v) = (v_0u - u_0v)^k H(u,v).$$

Demostración. Como $[u_0,v_0]\neq[0,0]$ (recordemos que esto no lo permitimos), supongamos sin pérdida de generalidad que $v_0\neq 0$. En caso contrario, la demostración sería análoga tomando u_0. Sea pues $m=grado(G)$ y sea $g(u)=G(u,v_0)$.

Observemos que si $g(u)\equiv 0$, entonces $g(u)=G(u,v_0)=\sum_{i=0}^m a_iu^iv_0^{m-i}=0$, y entonces $G(u,v)\equiv 0$, que está en contradicción con la hipótesis de la proposición.

Utilizando Ruffini, dividimos por la mayor potencia de $(u-u_0)$ que divide a $g(u)$ y obtenemos $g(u)=(u-u_0)^kh(u)$, para algún $k\geq 0$ y algún polinomio $h(x)=\sum_{i=k}^m b_{m-i}x^{m-i}$ con $h(u_0)\neq 0$, ya que hemos tomado la máxima potencia por la que podemos dividir. Sea $H(u,v)=\frac{v^{m-k}}{v_0^m}h(\frac{uv_0}{v})$. Vamos a ver que H es homogéneo de grado m-k:

$$H(u,v) = \sum_{i=k}^m b_{m-i}\left(\frac{uv_0}{v}\right)^{m-i}\frac{v^{m-k}}{v_0^m} = \sum_{i=k}^m b_{m-i}u^{m-i}v_0^{-i}v^{i-k}$$

luego cada monomio tiene grado $m-i+i-k=m-k$, por tanto H es homogéneo de grado m-k.

Además, por ser G homogéneo de grado m,

$$G(u,v) = v^mG\left(\frac{u}{v},1\right) = \frac{v^m}{v_0^m}G\left(\frac{uv_0}{v},v_0\right) = \left(\frac{v}{v_0}\right)^m g\left(\frac{uv_0}{v}\right) = \frac{v^m}{v_0^m}\left(\frac{uv_0}{v}-u_0\right)^k h\left(\frac{uv_0}{v}\right) =$$

$$= \frac{v^m}{v_0^m}(uv_0-vu_0)^k\frac{1}{v^k}h\left(\frac{uv_0}{v}\right) = \frac{v^{m-k}}{v_0^m}(uv_0-u_0v)^kh(\frac{uv_0}{v}) = (uv_0-u_0v)^kH(u,v).$$

□

Veamos ahora unos lemas que nos dan el valor del orden en caso de intersección o tangencia. Esto nos será útil para trabajar con él en las sucesivas demostraciones.

Lema 1.2.22. *Sea $S(u,v)\not\equiv 0$ un polinomio homogéneos de grado 3. Entonces $S(u,v)$ tiene como mucho 3 ceros $[u,v]\in\mathbb{P}^1(K)$ contando multiplicidades.*

Demostración. Factorizamos S a la mayor potencia de v, digamos v^k. Entonces $S(u,v)$ se anula con orden k en $[1,0]$ y $S(u,v)=v^kS_0(u,v)$ con $S_0(1,0)\neq 0$.

Como $S_0(u,1)$ es un polinomio de grado 3-k, puede tener como máximo 3-k ceros, contando multiplicidades (tendrá exactamente 3-k si el cuerpo sobre el que trabajamos es algebraicamente cerrado).

Todos los puntos $[u,v]\neq[1,0]$ pueden ser escritos de la forma $[u,1]$, dividiendo entre $v\neq 0$, luego $S_0(u,v)$ tiene como máximo 3-k ceros, y por tanto $S(u,v)$ tiene como mucho $k+3-k=3$ ceros en $\mathbb{P}^1(K)$. □

Lema 1.2.23. *Sean L_1 y L_2 dos rectas de $\mathbb{P}^2(K)$ que se cortan en un punto P. Si $L_1(x,y,z) = \alpha L_2(x,y,z)$ para cierta constante α, entonces $ord_{L_1,P}(L_2) = \infty$. En caso contrario, $ord_{L_1,P}(L_2) = 1$*

Demostración. Parametrizamos L_1 en función de (u,v) y sustituimos en L_2 obteniendo $\widetilde{L}_2(u,v)$. Sea P el punto correspondiente a $[u_0, v_0]$. Como $P \in L_1 \cap L_2$ se tiene que $\widetilde{L}_2(u_0, v_0) = 0$ y por tanto $\widetilde{L}_2(u,v) = \beta(v_0 u - u_0 v)$ con β constante.

Si $\beta \neq 0$ entonces $ord_{L_1,P}(L_2) = 1$, por definición de orden.

Si $\beta = 0$ tenemos que $L_1 \equiv L_2$ entonces $L_1 = \alpha L_2$, para algún α constante y $ord_{L_1,P}(L_2) = \infty$, ya que se intersecan en todos los puntos. □

Proposición 1.2.24. *Sean C, D dos curvas y L una recta. Entonces para cualquier punto P se cumple:*

1. $ord_{L,P}(CD) = ord_{L,P}(C) + ord_{L,P}(D)$,
2. $ord_{L,P}(C + D) \geq min(ord_{L,P}(C), ord_{L,P}(D))$.

Demostración. Ambas son obvias a partir de la definición:

1. Si $ord_{L,P}(C) = a$, entonces siguiendo la notación de la definición, $(t - t_0)^a$ es la mayor potencia de $(t - t_0)$ que divide a $\widetilde{f}(t)$, y si $ord_{L,P}(D) = b$, $(t - t_0)^b$ es la mayor potencia de $(t - t_0)$ que divide a $\widetilde{g}(t)$. Por tanto, $(t - t_0)^b (t - t_0)^a$ es la mayor potencia de $(t - t_0)$ que divide a $\widetilde{fg}(t)$.
2. Si $ord_{L,P}(C) = a$, entonces siguiendo la notación de la definición, $(t - t_0)^a$ es la mayor potencia de $(t - t_0)$ que divide a $\widetilde{f}(t)$, y si $ord_{L,P}(D) = b$, $(t - t_0)^b$ es la mayor potencia de $(t - t_0)$ que divide a $\widetilde{g}(t)$. Supongamos sin pérdida de generalidad, que $a < b$. Entonces $(t - t_0)^a$ divide a $\widetilde{f + g}(t)$ y por tanto, se tiene lo que queríamos.

□

Definición 1.2.25. Un punto P de una curva proyectiva con ecuación $F(x,y,z) = 0$ se dice que es **singular** si $F'_x(P) = F'_y(P) = F'_z(P) = 0$. En caso contrario se dice que es no singular. Una curva se dice no singular si no tiene puntos singulares.

Observación. Que una punto sea no singular, equivalente a la existencia de la recta tangente en ese punto, ya que recordemos la recta tangente en el punto $P = (x,y,z)$ a una curva dada por un polinomio F tiene la forma:

$$\frac{\partial F}{\partial x}(P)X + \frac{\partial F}{\partial y}(P)Y + \frac{\partial F}{\partial z}(P)Z = 0.$$

Lema 1.2.26. *Si $F(x,y,z) = 0$ define una curva C y P es un punto no singular de C, entonces existe una única recta en $\mathbb{P}^2(K)$ que corta a C con orden al menos 2 en P, y es la tangente a C en P.*

Demostración. Sea L una recta que corta a C con orden $k \geq 1$. Parametrizamos L de la forma (1.17) y sustituimos en F obteniendo $\widetilde{F}(u,v) = F(a_1 u + b_1 v, a_2 u + b_2 v, a_3 u + b_3 v)$. Sea $[u_0, v_0]$ el punto correspondiente a P, es decir, $P = (a_1 u_0 + b_1 v_0, a_2 u_0 + b_2 v_0, a_3 u_0 + b_3 v_0)$.

Usando la Proposición 1.2.21 tenemos que $\widetilde{F}(u,v) = (v_0 u - u_0 v)^k H(u,v)$, para algún polinomio $H(u,v)$ con $H(u_0, v_0) \neq 0$. Por tanto:

$$\widetilde{F}_u(u,v) = k v_0 (v_0 u - u_0 v)^{k-1} H(u,v) + (v_0 u - u_0 v)^k H_u(u,v),$$

$$\widetilde{F}_v(u,v) = -k u_0 (v_0 u - u_0 v)^{k-1} H(u,v) + (v_0 u - u_0 v)^k H_v(u,v).$$

Teniendo en cuenta que $k \geq 1$, tenemos dos casos:

Si $k \geq 2$ entonces $\widetilde{F}_v(u_0, v_0) = \widetilde{F}_u(u_0, v_0) = 0$.

Si $k = 1$ entonces $\widetilde{F}_v(u_0, v_0) = v_0$ y $\widetilde{F}_u(u_0, v_0) = u_0$. Como $[u_0, v_0] \in \mathbb{P}^1(K)$, $u_0 \neq 0$ ó $v_0 \neq 0$, con lo que $(\widetilde{F}_u(u_0, v_0), \widetilde{F}_v(u_0, v_0)) \neq (0,0)$.

Por tanto, $k \geq 2$ si y solo si $\widetilde{F}_v(u_0, v_0) = \widetilde{F}_u(u_0, v_0) = 0$. Usando la regla de la cadena, tenemos que

$$\begin{aligned} \widetilde{F}_u(u_0, v_0) &= a_1 F_x(P) + a_2 F_y(P) + a_3 F_z(P) = 0, \\ \widetilde{F}_v(u_0, v_0) &= b_1 F_x(P) + b_2 F_y(P) + b_3 F_z(P) = 0. \end{aligned} \tag{1.18}$$

Observemos que como L es una recta dada por la ecuación $Ax + By + Cz = 0$, con $a = (a_1, a_2, a_3)$ y $b = (b_1, b_2, b_3)$ base de L, entonces las ecuaciones (1.18) solo se anulan si $(F_x(P), F_y(P), F_z(P)) \sim (A, B, C)$, con lo que la recta tangente a C en P, que recordemos que era $F_x(P)x + F_y(P)y + F_z(P)z = 0$, es la única que cumple que $\widetilde{F}_u(u_0, v_0) = \widetilde{F}_v(u_0, v_0) = 0$. □

1.2.4. Puntos singulares

Otro concepto que vamos a necesitar manejar es el de punto de inflexión y el de puntos singulares.

Definición 1.2.27. Un **punto de inflexión** de F es un punto no singular P tal que $ord_{T_p(F),P}(F) > 2$, donde $T_p(F)$ es la recta tangente a F en P.

Definición 1.2.28. Dado un polinomio $F \in K[x, y, z]$ y un punto $P \in F(K)$, se define el **Hessiano** de la siguiente manera:

$$H_P(F) = \begin{pmatrix} F''_{x^2}(P) & F''_{xy}(P) & F''_{xz}(P) \\ F''_{xy}(P) & F''_{y^2}(P) & F''_{yz}(P) \\ F''_{xz}(P) & F''_{yz}(P) & F''_{z^2}(P) \end{pmatrix}$$

Proposición 1.2.29. *Sea $F \in K[x, y, z]$ un polinomio de grado $d \geq 2$, y sea $P \in F(K)$ no singular. Entonces son equivalentes:*

1. *P es un punto de inflexión de F.*
2. *$T_p(F)$ divide a $(x, y, z)H_p(F)\begin{pmatrix} x \\ y \\ z \end{pmatrix}$*

En tal caso se cumple que

3. *$Det(H_p(F)) = 0$, donde H es el hessiano.*

Además, si $car(K)$ no divide a $d - 1$, entonces 1 es equivalente a 3.

Capítulo 2

El grupo de las curvas elípticas

2.1. Definición

Una vez establecidos estos conceptos previos, podemos dar paso a la definición de curva elíptica:

Definición 2.1.1. Una **curva elíptica** E es una curva proyectiva irreducible no singular de grado 3.

Veamos como podemos reducir esta definición a una curva más específica después de un cambio de coordenadas:

Tomemos $F \in K[x,y,z]$ cúbico, $F = \sum_{i+j+k=3} a_{x^i y^j z^k} x^i y^j z^k$. Vamos a tomar el punto $P = (0,1,0)$ y vamos a exigirle que $P \in F(K)$. Si evaluamos en P, solo nos queda a_{y^3}, y como queremos que se anule, pedimos que

$$a_{y^3} = 0.$$

Como queremos que F sea no singular, tiene que tener recta tangente en P, $T_P(F)$. Vamos a ver que salvo un cambio de coordenadas $T_P(F) = z$, es decir, que la recta tangente a F en P es la recta del infinito. Para ello, consideramos el cambio de coordenadas $\phi(X,y,z) = (z,x,y)$ que hace $\phi(P) = \phi(0,1,0) = (0,0,1)$. Obtenemos así un nuevo polinomio $F^\phi(x,y) = F\phi^{-1}(x,y,1) = F(y,1,x) = f_1 + (cosas\ de\ grado \geq 2) = a_{y^2 z}x + a_{xy^2}y + (cosas\ de\ grado \geq 2)$. Y si queremos que no sea singular, necesariamente $a_{y^2 z} \neq 0$ ó $a_{xy^2} \neq 0$.

De esta manera, si $T_P(F) = f_1 \circ \phi(x,y,z) = f_1(z,x,y) = a_{y^2 z}z + a_{xy^2}x = z$, entonces

$$a_{xy^2} = 0,$$

y por tanto

$$a_{y^2 z} \neq 0.$$

Luego de momento ya tenemos que nuestra curva elíptica pasa por el punto $(0,1,0)$ y que su tangente en ese punto es la recta del infinito.

Ahora le vamos a pedir que P sea un punto de inflexión. Llamemos $L = z$ a la recta tangente en P. Entonces $L^\phi = L\phi^{-1} = L(y,1,x) = x$. Si parametrizamos la recta $x = 0$ como $\alpha(t) = (0,t)$, tenemos que $F^\phi(\alpha(t)) = F\phi^{-1}(0,t,1) = F(t,1,0) = a_{x^3}t^3 + a_{x^2 y}t^2$. Como queremos que P sea un punto de inflexión, su multiplicidad debe ser 3 ó más, y por tanto

$$a_{x^2 y} = 0.$$

De esta forma nos queda

$$F^\phi(x,y) = a_{x^3}x^3 + a_{x^2 z}x^2 z + a_{xz^2}xz^2 + a_{z^3}z^3 + a_{xyz}xyz + a_{y^2 z}y^2 z + a_{yz^2}yz^2.$$

Por último queremos que a_{x^3} y $a_{y^2 z}$ sean opuestos y no nulos. Así, podemos dividir por a_{x^3} y que aparezca 1 y -1. Para ello hacemos un nuevo cambio de coordenadas, pero debemos tener

cuidado con los cambios que hagamos ahora, puesto que no deben modificar las condiciones que ya tenemos. No pueden mover la recta del infinito ni nuestro punto $[0,1,0]$. Tomamos pues, $\phi^{-1}(x,y,z) = (t^{-1}x, t^{-1}y, z)$. Entonces $F \circ \phi^{-1} = \sum_{i+j+k=3} a_{x^i y^j z^k} t^{-i} x^i t^{-j} y^j z^k = \sum_{i+j+k=3} c_{x^i y^j z^k} x^i y^j z^k$. Como queremos que $c_{x^3} = t^{-3} a_{x^3} = -c_{y^2 z} = -t^{-2} a_{y^2 z}$, tomamos $t = \dfrac{-a_{x^3}}{a_{y^2 z}}$, hacemos el cambio de variable, dividimos por a_{x^3}, y ya podemos suponer que $a_{x^3} = -1$ y $a_{y^2 z} = 1$.

Finalmente, renombrando los coeficientes obtenemos la ecuación

$$y^2 z + a_1 xyz + a_3 yz^2 = x^3 + a_2 x^2 z + a_4 xz^2 + a_6 z^3,$$

que deshomogeneizándola, da sentido a la siguiente definición:

Definición 2.1.2. Sean K un cuerpo y $a_1, a_2, a_3, a_4, a_6 \in K$. Una curva elíptica E sobre K es una curva proyectiva no singular, admitiendo una ecuación definida sobre K, denominada **ecuación de Weierstrass generalizada**

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \tag{2.1}$$

junto con un punto O que se denomina **punto del infinito**.

Observación. El punto del infinito, denotado O ó ∞ se considerará situado en lo alto del eje y. Así, una recta pasará por el infinito cuando sea vertical. En el desarrollo anterior, corresponde al punto $P = [0,1,0]$.

Proposición 2.1.3. *Sea K un cuerpo con $char(K) \neq 2, 3$.Entonces la ecuación (2.1) es equivalente a*

$$y^2 = x^3 + Ax + B, \tag{2.2}$$

*con $A, B \in K$. Esta ecuación se denomina **ecuación de Weierstrass simplificada**.*

Demostración. Partiendo de la ecuación generalizada (2.1) podemos dividir entre 2 y completar cuadrados:

$$\left(y + \frac{a_1 x}{2} + \frac{a_3 x}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right) x^2 + \left(a_4 + \frac{a_1 a_3}{2}\right) x + \left(a_6 + \frac{a_3^2}{4}\right).$$

Haciendo un cambio de variable

$$y_1 = y + \frac{a_1 x}{2} + \frac{a_3 x}{2}$$

y poniendo

$$a_2' = a_2 + \frac{a_1^2}{4},$$
$$a_4' = a_4 + \frac{a_1 a_3}{2},$$
$$a_6' = a_6 + \frac{a_3^2}{4},$$

obtenemos

$$y_1^2 = x^3 + a_2' x^2 + a_4' x + a_6'.$$

Como $char(K) \neq 3$ podemos completar cubos tomando $x_1 = x + \dfrac{a_2'}{3}$ obteniendo:

$$y_1^2 = x_1^3 + Ax_1 + B,$$

que es lo que queríamos.

□

Observación. Consideremos la curva elíptica E dada por (2.1). Veamos qué puntos de E están en el infinito. Para ello, hacemos $z = 0$ y obtenemos $x^3 = 0$, luego $x = 0$ y por tanto $[0, 1, 0]$ es el único punto de E que está en el infinito (este es nuestro punto del infinito). De esta manera se tiene que las rectas que pasan por $[0, 1, 0]$ son las de ecuación $Ax + Bz = 0$ con $(A, B) \neq (0, 0)$, es decir, la recta del infinito $z = 0$ y las que en coordenadas afines tienen la forma $x = x_0$, o sea, las rectas verticales.

Proposición 2.1.4. *Sea una curva C no singular cúbica sobre K definida por $F(x, y, z) = 0$ y sea L una recta. Entonces $\sum_{P\in\mathbb{P}^2(K)} ord_{L,P}(F)$ es 0, 1 ó 3.*

Demostración. Como F es no singular, $ord_{L,P}(F) \neq \infty$ para todo $P \in \mathbb{P}^2(K)$.

Si $L \cap F = 0$, entonces $\sum_{P\in\mathbb{P}^2(K)} ord_{L,P}(F) = 0$, luego consideremos $P_0 \in L \cap F$. Podemos suponer sin pérdida de generalidad (mediante un cambio de coordenadas), que $P_0 = [0, 1, 0]$ y que que la recta tangente a F en P es la recta del infinito $z = 0$. Repitiendo el proceso de obtención de (2.1), llegamos a

$$F(x, y, z) = \sum_{i+j+k=3} a_{x^i y^j z^k} x^i y^j z^k = a_{y^2 z} y^2 z + a_{xyz} xyz + a_{x^2 y} x^2 y + a_{x^3} x^3 + a_{x^2 z} x^2 z + a_{xz^2} xz^2 + a_{z^3} z^3.$$

Si hacemos la intersección con la recta del infinito nos queda

$$F(x, y, 0) = a_{x^2 y} x^2 y + a_{x^3} x^3. \tag{2.3}$$

Vamos a considerar las siguientes posibilidades para L:

- $L = z$: Si $a_{x^3} = a_{x^2 y} = 0$, entonces z divide a F y por tanto F es singular, en contradicción con las hipótesis. Así pues, uno de los dos es distinto de cero.
  - Si $a_{x^2 y} =$ necesariamente $a_{x^3} \neq 0$ y entonces, como vimos en la obtención de (2.1), P_0 es un punto de inflexión. Como $ord_{L,P_0}(F) \not> 3$ para una cúbica, tenemos que $ord_{L,P_0}(F) = 3$. Como (2.3), con las condiciones impuestas no puede anularse sin que x se anule, no hay más puntos en $L \cap F$, luego $L \cap F$ contiene solo a P_0 con orden 3, y por tanto $\sum_{P\in\mathbb{P}^2(K)} ord_{L,P}(F) = 3$.
  - Si $a_{x^3} = 0$, entonces como vimos en la obtención de (2.1), P_0 no es un punto de inflexión, es decir que $ord_{L,P_0}(F) = 2$. Consideramos $P_1 = [1, t, 0] \in L$. Sustituyendo en (2.3) obtenemos $F(P_1 = a_{x^2 y} t + a_{x^3}$, y por tanto $L \cap F = \left\{P_0, \left[1, \frac{-a_{x^2 y}}{a_{x^3}}, 0\right]\right\}$. Tenemos que $ord_{L,P_1}(F) \not> 2$, pero como $P_1 \in L \cap F$, no puede ser dos, y necesariamente $ord_{L,P_1}(F) = 1$. Por tanto $\sum_{P\in\mathbb{P}^2(K)} ord_{L,P}(F) = 3$.
- $L \neq z$: Como L pasa por $P_0 = [0, 1, 0]$ y no es la recta tangente, $ord_{L,P_0}(F) = 1$. Si $L \cap F = \{P_0\}$ entonces $\sum_{P\in\mathbb{P}^2(K)} ord_{L,P}(F) = 1$. Supongamos pues que existe $P_1 \neq P_0$, $P_0 \in L \cap F$. Escribimos $P_1 = [x_0, y_0, 1]$. Utilizamos la homografía

$$\phi = \begin{pmatrix} 1 & 0 & -x_0 \\ 0 & 1 & -y_0 \\ 0 & 0 & 1 \end{pmatrix}, \tag{2.4}$$

que mantiene la recta del infinito y P_0 pero cambia $\phi(P_1) = [0, 1, 0]$. De esta forma L, que pasa por P_0 y P_1, es $L = x$. Parametrizamos L como $\alpha(t) = (0, t)$ y sustituimos en F^ϕ teniendo en cuenta que la curva tiene que pasar por $P_1 = [0, 0, 1]$. Obtenemos

$$F(0, t, 1) = t(a_{y^2 z} t + a_{yz^2} \tag{2.5}$$

Necesariamente $a_{y^2 z} \neq 0$, como vimos en la obtención de (2.1).

- Si $a_{yz^2} = 0$ entonces $L \cap F = \{P_0, P_1\}$, y por tanto (2.5) nos da que $ord_{L,P_1}(F) = 2$. Así, $\sum_{P\in\mathbb{P}^2(K)} ord_{L,P}(F) = 1 + 2 = 3$.

- Si $a_{yz^2} \neq 0$, entonces (2.5) nos dice que $ord_{L,P_1}(F) = 1$ y que también existe el punto $P_2 = \left[0, \frac{-a_{yz^2}}{a_{y^2z}}, 1\right] \in L \cap F$. Puedo intercambiar los papeles de P_1 y P_2, llegando a que $ord_{L,P_2}(F) = 1$. Así, $\sum_{P \in \mathbb{P}^2(K)} ord_{L,P}(F) = 1 + 1 + 1 = 3$.

□

Citamos también el Teorema de Hasse, un importante resultado que nos permite dar una cota superior al número de puntos de una curva elíptica.

Teorema 2.1.5 (Hasse)**.** *Si E es una curva elíptica sobre el cuerpo F_q, de q elementos entonces*

$$||E| - q - 1| \leq 2\sqrt{q}.$$

2.2. Suma de puntos

La finalidad de esta sección es demostrar que las curvas elípticas forman un grupo abeliano. Para ello necesitamos definir una operación de suma y demostrar las propiedades pertinentes. A partir de ahora la notación $P = (x, y)$ denotará un punto afín de la curva elíptica E.

Si tenemos dos puntos P, Q pertenecientes a una curva elíptica dada por la ecuación (2.1),llamémosle F, podemos trazar la recta L que contiene a P y Q (si $P = Q$, es la recta tangente). Si $P \neq Q$, la Proposición 2.1.4 nos dice que existe un tercer punto en $F \cap L$. Vamos a definir como R ese tercer punto. En el caso en que $P = Q$, la recta L es la recta tangente a F en P. Por el Lema 1.2.26, tenemos que $ord_{L,P}(F) \geq 2$ y la Proposición 2.1.4 nos dice que existe un tercer punto en $F \cap L$ si contamos multiplicidades. Este tercer punto será P si P es un punto de inflexión de F, y será un punto diferente si no lo es. En cualquier caso, lo denotaremos también R. Definiremos $P + Q = -R$ como el simétrico de R con respecto al eje x, o lo que es lo mismo, la intersección de la curva con la recta que pasa por el punto del infinito y R.

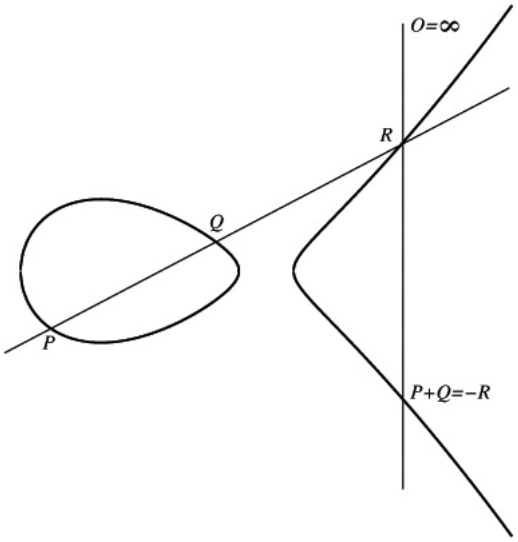

Figura 2.1: Suma de puntos. **Fuente**: [7]

Proposición 2.2.1. *Sea E una curva elíptica definida por la ecuación (2.1). Sean $P_1 = (x_1, y_1)$ y $P_2 = (x_2, y_2)$ puntos de E con $P_1, P_2 \neq \infty$. Entonces $P_1 + P_2 = P_3 = (x_3, y_3)$ donde*

$$x_3 = m^2 + a_1 m - a_2 - x_1 - x_2, \quad y_3 = -(m + a_1)x_3 - b - a_3,$$

siendo

$$m = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \text{ si } P_1 \neq P_2, \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} \text{ si } P_1 = P_2, \end{cases}$$

$$b = \begin{cases} \dfrac{y_1x_2 - y_2x_1}{x_2 - x_1} \text{ si } P_1 \neq P_2, \\ \dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} \text{ si } P_1 = P_2. \end{cases}$$

Además se cumple que $P + \infty = P$ para cualquier $P \in E$.

Demostración. Vamos a comenzar calculando la recta que pasa por P_1 y P_2, $y = mx + b$.

Si $P_1 \neq P_2$, podemos calcular sin ningún problema la pendiente de la recta L que une P_1 con P_2,

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

y el término independiente sustituyendo (x, y) por las coordenadas de p_2,

$$b = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}.$$

Si $P_1 = P_2$, la recta que pasa por ambos puntos es la tangente a la curva en P_1. Calculamos la pendiente $m = \frac{dy}{dx}$ derivando implícitamente (2.1):

$$2yy' + a_1xy' + a_1y + a_3y' = 3x^2 + 2a_2x + a_4.$$

Sustituyendo $m = y'$ y $(x_1, y_1) = P_1$, nos queda

$$m = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}.$$

Obtenemos la recta que queremos $y = mx+b$ a partir de la recta tangente $y-y_1 = m(x-x_1)$. Despejando, $y = mx + (y_1 - mx_1)$ y por tanto $b = y_1 - mx_1$. Es decir,

$$b = \frac{2y_1^2 + a_1x_1y_1 + a_3y_1 - 3x_1^3 - 2a_2x_1^2 - a_4x_1 + a_1x_1y_1}{2y_1 + a_1x_1 + a_3}$$

y sustituyendo y_1^2 por la correspondiente expresión en (2.1), obtenemos finalmente que

$$b = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}.$$

Una vez que tenemos la recta que pasa por ambos puntos, estamos en disposición de calcular P_3. Denotemos $F(x, y) = 0$ a la ecuación (2.1) igualada a cero. La intersección de la curva con la recta que pasa por P_1 y P_2, $y = mx + b$, se obtiene haciendo $F(x, mx + b) = 0$. Luego las coordenadas x de P_1, P_2 y P_3 serán las raíces de esa expresión, es decir

$$F(x, mx + b) = (x - x_1)(x - x_2)(x - x_3).$$

Sustituyendo la expresión de F, tenemos

$$x^3 + a_2x^2 + a_4x + a_6 - (mx + b)^2 - a_1x(mx + b) - a_3(mx + b) = x^3 - (x_1 + x_2 + x_3)x^2 + R,$$

donde R son términos de grado inferior. Identificando coeficientes obtenemos

$$a_2 - m^2 - a_1m = -(x_1 + x_2 + x_3),$$

y por tanto,

$$x_3 = m^2 + a_1m - a_2 - x_1 - x_2,$$
$$y_3 = -(m + a_1)x_3 - b - a_3.$$

Por último, supongamos que uno de los dos puntos es ∞. Entonces la recta L que pasa por P_1 y $P_2 = \infty$ es vertical. Haciendo $L \cap E$ obtenemos P_1' y calculando el simétrico con respecto al eje x, como L es vertical, obtenemos justamente P_1, luego efectivamente $P_1 + \infty = P_1$ para todo $P_1 \in E$.

□

Veamos ahora el caso en que $char(K)$ no es dos ni tres, siendo K el cuerpo donde está definida la curva. Esto nos permite usar la definición de curva elíptica con la ecuación simplificada de Weierstrass y obtener unas fórmulas más simples para la suma de puntos:

Proposición 2.2.2. *Sea E una curva elíptica definida por la ecuación (2.2). Sean* $P_1 = (x_1, y_1)$ *y* $P_2 = (x_2, y_2)$ *puntos de E con* $P_1, P_2 \neq \infty$. *Entonces si* $x_1 = x_2$ *pero* $y_1 \neq y_2$ *ó* $P_1 = P_2$ *e* $y_1 = 0$, *entonces* $P_1 + P_2 = \infty$. *En otro caso,* $P_1 + P_2 = P_3 = (x_3, y_3)$, *con* $x_3 = m^2 - 2x_1$, $y_3 = m(x_3 - x_1) - y_1$, *donde*

$$m = \begin{cases} \dfrac{3x_1^2 + A}{2y_1} \text{ si } x_1 = x_2, \\ \dfrac{y_2 - y_1}{x_2 - x_1} \text{ si } x_1 \neq x_2. \end{cases}$$

Demostración. Si $x_1 \neq x_2$, podemos calcular sin ningún problema la pendiente de la recta L que une P_1 con P_2:

$$m = \frac{y_2 - y_1}{x_2 - x_1},$$

luego la ecuación de L es $y = m(x - x_1) + y_1$. Calculamos la intersección de L con la curva E sustituyendo la ecuación de L en la de E y desarrollamos

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B,$$

$$x^3 - m^2x^2 - (2m - A - 2x_1m^2)x - (m^2x_1^2 + y_1^2 - 2mx_1 - B) = 0.$$

Esta ecuación no es fácil de resolver. Sin embargo, podemos usar las fórmulas de Cardano-Vietta para calcular la raíz que nos falta. La otras dos raíces son las coordenadas x de P_1 y P_2. Tenemos pues, que

$$x_1 + x_2 + x_3 = -m^2(-1) = m^2,$$

luego $x_3 = m^2 - x_1 - x_2$ y sustituyendo $y_3 = m(x_1 - x_3) + y_1$. Finalmente, haciendo la simetría de y_3 con respecto al eje x, se obtiene $y_3 = m(x_3 - x_1) - y_1$.

Si $P_1 = P_2$ pero $y_1 \neq 0$, la recta que pasa por ambos puntos es la recta tangente. Calculamos la pendiente de la tangente de manera usual, calculando la derivada:

$$y^2 = x^3 + Ax + B,$$

$$2y\frac{dy}{dx} = 3x^2 + A,$$

luego,

$$m = \frac{dy_1}{dx_1} = \frac{3x_1^2 + A}{2y_1}.$$

Por tanto L viene dada por la ecuación $y = m(x - x_1) + y_1$. Haciendo la intersección con E:

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B,$$

$$x^3 - m^2x^2 - (2m - A - 2x_1m^2)x - (m^2x_1^2 + y_1^2 - 2mx_1 - B) = 0.$$

Podemos volver a utilizar Cardano Vietta, ya que aunque solo conocemos una raíz, x_1, es una raíz doble. De esta manera obtenemos, ya haciendo la simetría

$$x_1 + x_1 + x_3 = -m^2(-1) = m^2,$$

$$x_3 = m^2 - 2x_1,$$

$$y_3 = m(x_1 - x_3) - y_1.$$

Si $x_1 = x_2$ pero $y_1 \neq y_2$, la recta L que une P_1 y P_2 es vertical, luego cortará a la curva en el infinito. Haciendo el simétrico de ∞ respecto al eje x, obtenemos el mismo punto ∞, y como hemos considerado el ∞ en los dos extremos del eje y, tenemos que $P_1 + P_2 = \infty$.

Si $P_1 = P_2$ e $y_1 = 0$, la recta L sería una recta vertical (la pendiente se hace infinita) y por el mismo razonamiento que en el caso anterior, se obtiene que $P_1 + P_2 = \infty$. □

Proposición 2.2.3. *La suma de puntos definida anteriormente, cumple las siguientes propiedades:*

(Conmutatividad) $P_1 + P_2 = P_2 + P_1$ *para todo* $P_1, P_2 \in E$.

(Elemento neutro) $P + \infty = P$ *para todo* $P \in E$.

(Elemento inverso) Dado $P \in E$, *existe* $P' \in E$ *tal que* $P + P' = \infty$. *Este punto* P' *suele denotarse* $-P$.

(Asociatividad) $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ *para todo* $P_1, P_2, P_3 \in E$.

Demostración. La propiedad comutativa es inmediata, ya que la recta que va de P_1 a P_2 es la misma que la que va de P_2 a P_1.

La propiedad del elemento neutro se tiene por la definición de la suma, ya que vimos que $P + \infty = P$.

Para la propiedad del elemento inverso, si P' es el simétrico de $P \neq \infty$ con respecto al eje x, como la recta que los une es vertical, $P' + P = \infty$, y queda demostrado. En el caso $P = \infty$, tenemos por la definición de la suma que $\infty + \infty = \infty$.

La demostración de la asociatividad requiere más trabajo, por lo que le dedicaremos una sección completa.

□

Observación. Hay que tener cuidado a la hora de calcular $-P$. Si $P = (x_0, y_0)$, y la curva viene dada con la ecuación simplificada de Wieierstrass, $-P = (x_0, -y_0)$, ya que la curva es simétrica con respecto al eje x. Sin embargo esto es muy diferente cuando se usa la ecuación generalizada de Weierstrass. En este caso, para encontrar $-P$, hay que calcular la intersección de la curva con la recta vertical que pasa por P, es decir $x = x_0$. Tenemos pues,

$$y + a_1 x_0 y + a_3 y = x_0^3 + a_2 x_0^2 + a_4 x_0 + a_6.$$

Esta ecuación no es fácil de resolver, pero usando Cardano-Vietta y conociendo una de las soluciones, y_0, tenemos:

$$y + y_0 = -a_1 x_0 - a_3,$$

$$y = -a_1 x_0 - a_3 - y_0,$$

luego si $P = (x_0, y_0)$, se tiene que $-P = (X_0, -a_1 x_0 - a_3 - y_0)$.

2.3. La asociatividad

Consideremos una curva elíptica E y los puntos $P, Q, R \in E$. Para evitarnos simetrías, en vez de probar la igualdad $(P+Q)+R = P+(Q+R)$, probaremos que $-((P+Q)+R) = -(P+(Q+R))$. Para calcular $-((P+Q)+R)$ (Figuras 2.2, 2.4 y 2.6) y $-(P+(Q+R))$ (Figuras 2.3, 2.5 y 2.7) necesitamos calcular las rectas

$$\begin{array}{lll} l_1 = \overline{PQ}, & m_2 = \overline{\infty, P+Q}, & l_3 = \overline{R, P+Q}, \\ m_1 = \overline{QR}, & l_2 = \overline{\infty, Q+R}, & m_3 = \overline{P, Q+R}, \end{array} \tag{2.6}$$

y ver dónde se cortan.

Definimos de esta manera

$$P_{ij} = l_i \cap m_j \;\; i, j = 1, 2, 3. \tag{2.7}$$

Proposición 2.3.1. $P_{ij} \in E$ *para todo* $(i, j) \neq (3, 3)$, $\;i, j = 1, 2, 3$

Demostración. Vamos a ver que efectivamente cada punto está en la curva:

$P_{11} = l_1 \cap m_1 = \overline{PQ} \cap \overline{QR} = Q \in E$,

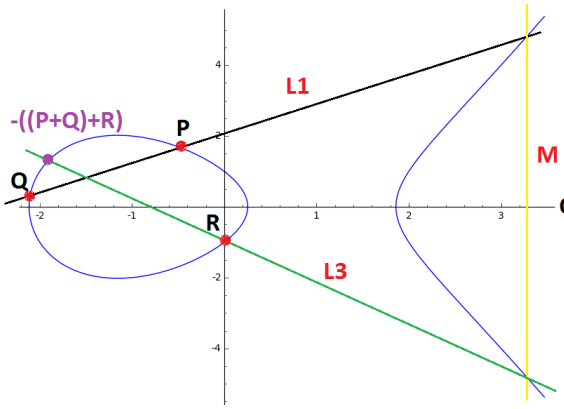

Figura 2.2: $-((P+Q)+R)$

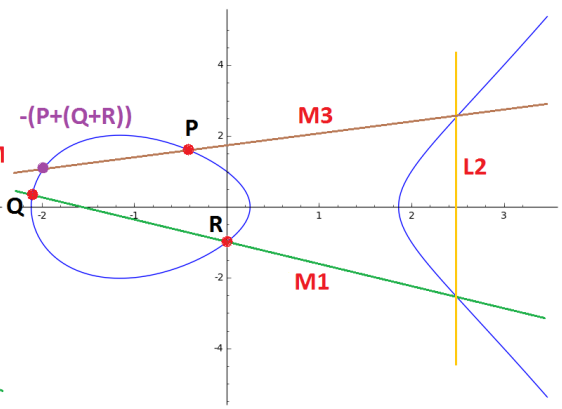

Figura 2.3: $-(P+(Q+R))$

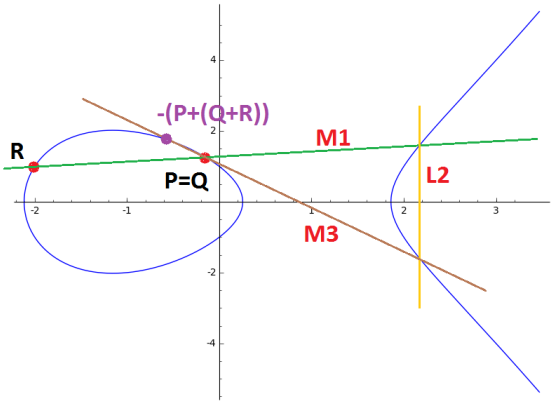

Figura 2.4: $-((P+Q)+R)$, con $P=Q$

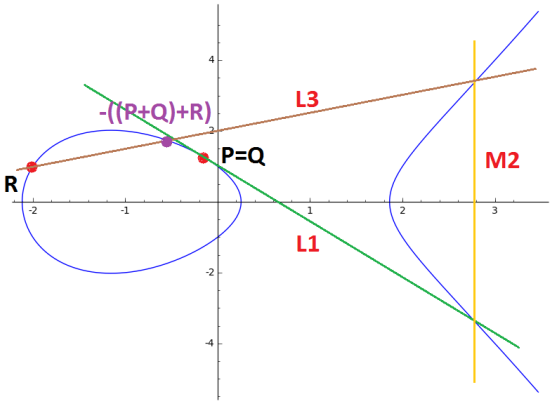

Figura 2.5: $-(P+(Q+R))$, con $P=Q$

$P_{12} = l_1 \cap m_2 = \overline{PQ} \cap \overline{\infty, P+Q} = -(P+Q) \in E,$
$P_{13} = l_1 \cap m_3 = \overline{PQ} \cap \overline{P, Q+R} = P \in E,$
$P_{21} = l_2 \cap m_1 = \overline{\infty, Q+R} \cap \overline{QR} = -(Q+R) \in E,$
$P_{22} = l_2 \cap m_2 = \overline{\infty, Q+R} \cap \overline{\infty, P+Q} = \infty \in E,$
$P_{23} = l_2 \cap m_3 = \overline{\infty, Q+R} \cap \overline{P, Q+R} = Q+R \in E,$
$P_{31} = l_3 \cap m_1 = \overline{R, P+Q} \cap \overline{QR} = R \in E,$
$P_{32} = l_3 \cap m_2 = \overline{R, P+Q} \cap \overline{\infty, P+Q} = P+Q \in E.$

□

El único punto del que no podemos decir nada, es P_{33}. Para demostrar que este punto efectivamente está en la curva, necesitaremos el concepto de orden de intersección y una serie de lemas que nos servirán para probarlo. Luego los pasos que seguiremos para demostrar la asociatividad serán ver que $P_{33} \in E$, estudiar los casos que nos podemos encontrar como que algún punto $P_{ij} = \infty$, algunas rectas m_i y l_i sean iguales o que sean tangentes a la curva y deducir que estemos en el caso que estemos, siempre se cumple la asociatividad.

2.3.1. Preparatorio

La clave para demostrar que P_{33} está en la curva es el siguiente Teorema:

Teorema 2.3.2. *Sea $C(x,y,z)$ un polinomio cúbico homogéneo que describe una curva C en $\mathbb{P}^2(K)$. Sean l_1, l_2, l_3 y m_1, m_2, m_3 rectas en $\mathbb{P}^2(K)$ tales que $l_i \neq m_j$ para todo $i,j = 1,2,3$. Sea $P_{ij} = l_i \cap m_j$. Supongamos que P_{ij} es un punto no singular en C para todo par $(i,j) \neq (3,3)$.*

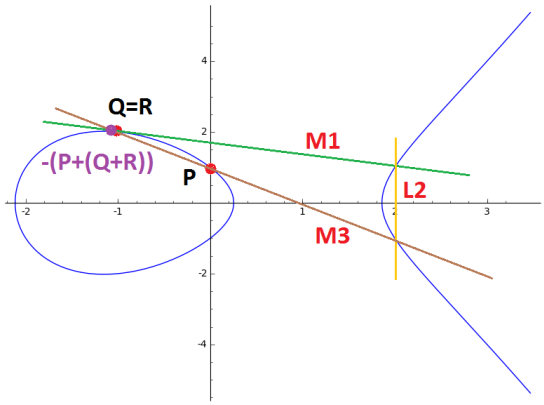

Figura 2.6: $-((P+Q)+R)$, con $Q=R$

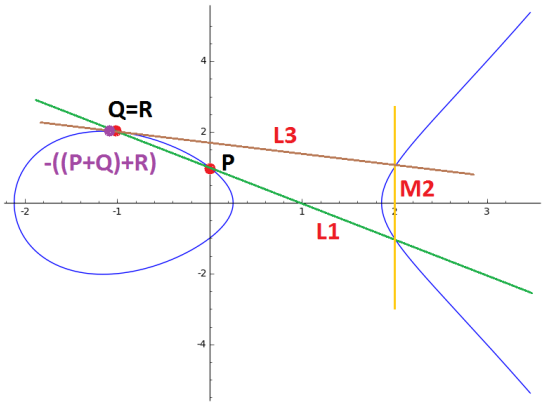

Figura 2.7: $-(P+(Q+R))$, con $Q=R$

Además, requerimos que si para algún i hay $k \geq 2$ puntos P_{i1}, P_{i2}, P_{i3} iguales, entonces l_i corte a C con orden al menos k en ese punto, y que si para algún j hay $k \geq 2$ puntos P_{1j}, P_{2j}, P_{3j} iguales, entonces m_j corte a C con orden al menos k en ese punto. Con estas hipótesis, se tiene que $P_{33} \in C$.

La demostración de este teorema no es nada trivial. De hecho, hemos extraído varios lemas que se utilizan durante todo el desarrollo, que se enunciarán tras acabar la demostración, de forma que sea más fácil de seguir y se tengan claros los puntos clave.

Demostración. Parametrizamos l_1 de la forma (1.17). Sustituyendo en $C(x,y,z)$ obtenemos $\widetilde{C}(u,v) = C(a_1u+b_1v, a_2u+b_2v, a_3u+b_3v)$. Como l_1 pasa por P_{11}, P_{12}, P_{13}, sean $[u_1,v_1],[u_2,v_2],[u_3,v_3]$ los parámetros en l_1 correspondientes a esos puntos. Como estos puntos están en C, se tiene que $\widetilde{C}(u_i,v_i) = 0$, para todo $i = 1,2,3$. Sea m_j con ecuación $d_jx+e_jy+f_jz=0$. Sustituyendo la parametrización de l_1 en la ecuación, obtenemos la ecuación de la intersección $m_j \cap l_1$, $\widetilde{m}_j(u,v)$. Como $P_{ij} \in m_j$, se tiene que $\widetilde{m}_j(u_j,v_j)=0$, $j=1,2,3$. Como $l_1 \neq m_j$ y los ceros de $\widetilde{m}_j$ son los puntos de $m_j \cap l_1$, $\widetilde{m}_j$ se anula solo en P_{1j}, por tanto $\widetilde{m}_j \not\equiv 0$, luego $\widetilde{m}_1(u,v)\widetilde{m}_2(u,v)\widetilde{m}_3(u,v) \not\equiv 0$ es un polinomio cúbico no nulo y homogéneo, que se anula en los puntos $[u_i,v_i]$ con $i=1,2,3$. Además, si k de los puntos P_{ij} son los mismos, entonces k de las funciones $\widetilde{m}_j$ con $j=1,2,3$ se anulan en ese punto, luego $\widetilde{m}_1(u,v)\widetilde{m}_2(u,v)\widetilde{m}_3(u,v)$ se anula con orden al menos k en dicho punto, es decir, $(v_iu-u_iv)^k$ divide a $\widetilde{m}_1(u,v)\widetilde{m}_2(u,v)\widetilde{m}_3(u,v)$. Por tanto, podemos aplicar el Lema 2.3.3 tomando $S = \widetilde{m}_1(u,v)\widetilde{m}_2(u,v)\widetilde{m}_3(u,v)$ y $R = \widetilde{C}$. Así, existe una constante $\alpha \neq 0$ tal que $\widetilde{C}(u,v) = \alpha\widetilde{m}_1(u,v)\widetilde{m}_2(u,v)\widetilde{m}_3(u,v)$. Llamemos $C_1(x,y,z) = C(x,y,z) - \alpha m_1(x,y,z)m_2(x,y,z)m_3(x,y,z)$.

Vamos a especificar más la parametrización de l_1. Esta recta es de la forma $l_1(x,y,z) = ax+by+cz=0$. Como al menos un coeficiente es no nulo, supongamos $a \neq 0$, podemos pasar a su forma paramétrica haciendo el cambio $y=u$, $z=v$ y despejando x, con lo que se tiene:

$$\begin{cases} x = -\dfrac{b}{a}u - \dfrac{c}{a}v, \\ y = u, \\ z = v, \end{cases} \tag{2.8}$$

que es equivalente a tomar $(a_1,a_2,a_3) = \left(-\frac{b}{a},1,0\right)$ y $(b_1,b_2,b_3) = \left(-\frac{c}{a},0,1\right)$ en las ecuaciones (1.2). Sustituyendo en C_1 tenemos $\widetilde{C}_1(u,v) = C_1(-\frac{b}{a}u - \frac{c}{a}v, u, v)$.

Observemos que usando Newton podemos escribir

$$x^n = \frac{1}{a^n}(ax)^n = \frac{1}{a^n}((ax+by+cz)-(by+cz))^n = \frac{1}{a^n}((ax+by+cz)^n + k_1(ax+by+cz)^{n-1}(by+cz)+\ldots$$

y por tanto podemos reordenar C_1 para que sea un polinomio en $(ax+by+cz)$ cuyos coeficientes

sean polinomios en $K[y,z]$:

$$C_1(x,y,z) = a_3(y,z)(ax+by+cz)^3 + a_2(y,z)(ax+by+cz)^2 + a_1(y,z)(ax+by+cz) + a_0(y,z).$$

Sustituyendo aquí la parametrización de l_1, como $ax+by+cz$ se anula exactamente cuando x,y,z se escriben en términos de u,v con la fórmula (2.8), tenemos que $\widetilde{C}_1(u,v) = 0 = a_0(u,v)$, luego $a_0(y,z) = a_0(u,v) = 0$. Por tanto,

$$C_1(x,y,z) = a_3(y,z)(ax+by+cz)^3 + a_2(y,z)(ax+by+cz)^2 + a_1(y,z)(ax+by+cz),$$

y entonces $C_1(x,y,z) = C(x,y,z) - \alpha m_1(x,y,z)m_2(x,y,z)m_3(x,y,z)$ es múltiplo de $l_1 = ax+by+cz$. Análogamente, volviendo a aplicar el Lema 2.3.3 con $S = \widetilde{l}_1(u,v)\widetilde{l}_2(u,v)\widetilde{l}_3(u,v)$ y $R = \widetilde{C}$ y repitiendo el proceso, tenemos que $C(x,y,z) - \beta l_1(x,y,z)l_2(x,y,z)l_3(x,y,z)$ es múltiplo de $m_1(x,y,z)$ para algún $\beta \in K \setminus \{0\}$. De esta manera tenemos que

$$D(x,y,z) = C - \alpha m_1(x,y,z)m_2(x,y,z)m_3(x,y,z) - \beta l_1(x,y,z)l_2(x,y,z)l_3(x,y,z)$$

es múltiplo de l_1 y m_1, y como $l_1 \neq m_1$, se tiene que $D(x,y,z) = l_1 m_1 l$, con $l(x,y,z)$ lineal o cero.

Por hipótesis, P_{22}, P_{23}, P_{32} son ceros de $C, l_1l_2l_3$ y $m_1m_2m_3$, por tanto también son ceros de D. Veamos que $D \equiv 0$. Si $l \equiv 0$, se tiene directamente que $D \equiv 0$, así que supongamos que $l \not\equiv 0$, es decir $l(x,y,z) = 0$ define una recta, y procedamos por reducción al absurdo:

1. $P_{32} \neq P_{22}$: Supongamos que $P_{32} = P_{22}$. En este caso, $ord_{m_2,P_{22}}(l_1m_1l) \geq 2$, y por el Lema 1.2.26tenemos que m_2 es tangente a C en P_{22}. Esto obliga a que $l = m_2$. Vamos a verlo:

   Como $P_{12} = l_1 \cap m_2$ y $P_{22} = l_2 \cap m_2$, si $m_1(P_{22}) = 0$, entonces $P_{21} = P_{22}$. Esto implica que $ord_{l_2,P_{22}}(C) \geq 2$ y por tanto l_2 es la recta tangente a C en P_{22}. Por la unicidad del Lema 1.2.26 se tendría $l_2 = m_2$, en contra de las hipótesis. Por tanto $m_1(P_{22}) \neq 0$, luego $ord_{m_2,P_{22}}(l_1l) = ord_{m_2,P_{22}}(l_1m_1l) \geq 2$. Si $l_1(P_{22}) \neq 0$ entonces $ord_{m_2,P_{22}}(l) \geq 2$ y eso implica que $l = m_2$, que es lo que queríamos. En caso contrario, $P_{22} \in l_1 \cap m_2 = P_{12}$, luego $P_{12} = P_{22} = P_{23}$, y por tanto $ord_{m_2,P_{22}}(C) \geq 3$. Como hemos probado que $m_1(P_{22}) \neq 0$ y estamos en la hipótesis de que $l_1(P_{22}) = 0$ pero $l_1 \neq m_2$, entonces $ord_{m_2,P_{22}}(l) \geq 2$ y por el Lema 1.2.26, $l = m_2$, como queríamos ver.
   Llegados a este punto, tenemos que si $P_{32} = P_{22}$ entonces $l = m_2$. Usando el Lema (2.3.5), $P_{23} \in l, m_2, l_2, m_3$ y por tanto $P_{22} = P_{23}$, lo que implica que l_2 es tangente a C en P_{22}. Como $P_{32} = P_{22}$ entonces m_2 es tangente a C en P_{22} y por la unicidad del Lema 1.2.26, necesariamente $l_2 = m_2$, lo que está en contradicción con las hipótesis, luego obligatoriamente $P_{32} \neq P_{22}$.

2. $P_{23} \neq P_{22}$: Es análogo al caso anterior, cambiando las m_i por l_i y viceversa.

3. $P_{23} = P_{22}$ ó $P_{22} = P_{32}$: Si no fuese así, l y l_2 serían ambas rectas (la única) que contienen a P_{23} y P_{22}, y por otro lado, l y m_2 serían rectas que contienen a P_{22} y P_{32}. Por tanto $l_2 = l = m_2$, en contra de las hipótesis.
   De esta manera, todas las posibilidades nos han llevado a contradicciones, lo que significa que $l(x,y,z) \equiv 0$ y por tanto, $D \equiv 0$, luego quedaría $C = \alpha l_1l_2l_3 + \beta m_1m_2m_3$, pero como l_3 y m_3 se anulan en P_{33} se tendría $C(P_{33}) = 0$, con lo que concluye la prueba de este teorema.

□

Pasamos a enunciar y demostrar los lemas que hemos ido utilizando en la demostración:

Lema 2.3.3. *Sea $R(u,v)$ y $S(u,v)$ polinomios homogéneos de grado 3. Supongamos que hay tres puntos $[u_i,v_i]$, con $i = 1,2,3$, no necesariamente distintos donde S y R se anulan. Supongamos que si k de esos puntos son iguales, R y S se anulan con orden al menos k en ese punto, es decir $(v_iu - u_iv)^k$ divide a R y S. Entonces existe una constante α tal que $R = \alpha S$.*

Demostración. Sea $[u_0, v_0] \in \mathbb{P}^1(K)$ cumpliendo que $[u_0, v_0] \neq [u_i, v_i]$ para todo $i = 1, 2, 3$. Por el Lema 1.2.22, S puede tener como mucho tres ceros y por tanto $[u_0, v_0]$ ya no puede ser raíz de S (sería una cuarta raíz), o sea $S(u_0, v_0) \neq 0$. Si consideramos $\alpha = \frac{R(u_0,v_0)}{S(u_0,v_0)}$ entonces $R(u, v) - \alpha S(u, v)$ es un polinomio homogéneo cúbico que se anula en los cuatro puntos $[u_i, v_i]$, con $i = 0, 1, 2, 3$ y por tanto se tiene que $R - \alpha S \equiv 0$, es decir, $R = \alpha S$.

□

Lema 2.3.4. *Si $P_{ij} = P_{ik}$ con $i, j, k \in \{1, 2, 3\}$ y $j \neq k$, entonces $ord_{l_i,P_{ij}}(C) \geq 2$. Además, $ord_{l_i,P_{ij}}(m_j m_k) \geq 2$ y $ord_{l_i,P_{ij}}(D) \geq 2$. Análogamente, si $P_{ji} = P_{ki}$ con $j \neq k$, entonces $ord_{m_i,P_{ji}}(D) \geq 2$.*

Demostración. Como $P_{ji} = P_{ki}$ y $P_{ki} \in m_i$ tenemos que $ord_{m_i,P_{ki}}(l_j) = ord_{m_i,P_{ki}}(l_k) = 1$, esto último por el Lema 1.2.26 y sabiendo que $l_j \neq m_i \neq l_k$. Por tanto, sumando tenemos que $ord_{m_i,P_{ki}}(\alpha l_j l_k l_i) \geq 2$. Sabemos que $ord_{m_i,P_{ki}}(\beta m_j m_k m_i) = \infty$, ya que tenemos intersección de m_i consigo misma. Como $D = C - \alpha m_1 m_2 m_3 - \beta l_1 l_2 l_3$ es suma de tres términos, que como acabamos de ver, cada uno se anula con orden al menos dos, se tiene que $ord_{m_i,P_{ki}}(D) \geq 2$. □

Lema 2.3.5. $l(P_{22}) = l(P_{23}) = l(P_{32}) = 0$

Demostración. Demostraremos que $l(P_{23}) = 0$, los otros casos son análogos.
Vamos a ver primero que $m_1(P_{23})l(P_{23}) = 0$. Para ello, analizamos dos situaciones:

1. Supongamos primero que $P_{13} \neq P_{23}$: Si esto ocurre, se tiene que $l_1(P_{23}) \neq 0$, ya que si fuese cero, se tendría que $P_{23} \in l_1$ además de que $P_{23} \in l_2, m_3$ por definición, luego $P_{23} = P_{13} = l_1 \cap m_3$ y esto sería una contradicción. Por tanto, como $D(P_{23}) = 0$ se tiene que $m_1(P_{23})l(P_{23}) = 0$.

2. Supongamos ahora que $P_{13} = P_{23}$: En este caso se tiene que por las hipótesis del Teorema 2.3.2 que $ord_{m_3,P_{23}}(C) \geq 2$ y por el Lema 1.2.26, m_3 es tangente a C en P_{23}. Además, como $P_{13} = P_{23}$, por el Lema 2.3.4 se tiene que $ord_{m_3,P_{23}}(D) \geq 2$. Pero $ord_{m_3,P_{23}}(l_1) = 1$, luego usando la segunda forma de describir D, es decir $D = l_1 m_1 l$, tenemos que $ord_{m_3,P_{23}}(m_1 l) = ord_{m_3,P_{23}}(D) - ord_{m_3,P_{23}}(l_1) \geq 1$ y por tanto $m_1(P_{23})l(P_{23}) = 0$.

Como en ambos casos $m_1(P_{23})l(P_{23}) = 0$, si $m_1(P_{23}) \neq 0$ entonces $l(P_{23}) = 0$, y ya hemos terminado. Así que supongamos que $m_1(P_{23}) = 0$, es decir, $P_{23} \in m_1$ (además de tener $P_{23} \in m_3, l_2$ por definición), por tanto como l_2 y m_1 se intersectan en un único punto, necesariamente $P_{23} = P_{21}$, y por el Lema 2.3.4 $ord_{l_2,P_{23}}(D) \geq 2$. Volviendo a usar la segunda forma de escribir D, se tiene que $ord_{l_2,P_{23}}(l_1 l) \geq 1$ y por tanto $l_1(P_{23})l(P_{23}) = 0$.

Si $l_1(P_{23}) = 0$, entonces $P_{23} \in l_1, l_2, m_3$, por tanto $P_{13} = P_{23}$, y por las hipótesis de 2.3.2, m_3 es tangente a C en P_{23} y P_{23} es un punto no singular de C, luego por el Lema 1.2.26, necesariamente $l_2 = m_3$ que está en contradicción con las hipótesis de 2.3.2. Luego la única opción es $l_1(P_{23}) \neq 0$ y por tanto $l(P_{23}) = 0$. □

2.3.2. Prueba de la asociatividad

Llegados a este punto, ya estamos en condiciones de probar la asociatividad. Para ello, consideremos la curva elíptica E y las rectas m_i, l_j definidas en (2.6). Estas rectas se intersectan en los puntos que se pueden ver en la tabla 2.1.

	l_1	l_2	l_3
m_1	Q	$-(Q+R)$	R
m_2	$-(P+Q)$	∞	$P+Q$
m_3	P	$Q+R$	X

Tabla 2.1: Intersecciones

Vamos a analizar todos los posibles casos para demostrar que la asociatividad se cumple en todos ellos. Primero trataremos los casos triviales, donde algún punto es ∞ o los puntos son colineales:

1. Al menos uno de los puntos P, Q, R es ∞: Entonces trivialmente se da la asociatividad, ya que el ∞ es el elemento neutro de la suma.

2. $P+Q = \infty$: Entonces $(P+Q)+R = \infty+R = R$. Por otro lado, para calcular la suma $Q+R$ se necesita la recta L a través de Q y R, que corta a E en $-(Q+R)$. Como $P+Q = \infty$, la reflexión de Q con respecto al eje x es P, luego la recta simétrica L' de L, pasa por $P, -R, Q+R$. La suma $P+(Q+R)$ se calcula con la recta que pasa por P y $Q+R$, que es precisamente L', luego el tercer punto de intersección con E es $-R$, y por tanto haciendo la simetría $P+(Q+R) = R$, y se cumple la asociatividad.

3. $Q+R = \infty$: Es análogo al anterior.

4. P, Q y R son colineales: En este caso la asociatividad es trivial, ya que al ser colineales trabajamos sobre la misma recta y solo pasamos de un punto de intersección a otro.

5. P, Q y $Q+R$ son colineales: Entonces $P+(Q+R) = -Q$ y $P+Q = -(Q+R)$, por tanto $(P+Q)+R = -(Q+R)+R$ y por el Lema 2.3.6 se cumple la asociatividad.

6. $P = R$: Entonces $(P+Q)+R = R+(P+Q) = P+(P+Q) = P+(R+Q) = P+(Q+R)$ y se cumple la asociatividad.

Lema 2.3.6. *Sean P_1, P_2 puntos de una curva elíptica. Entonces $(P_1+P_2)-P_2 = P_1$ y $-(P_1+P_2)+P_2 = -P_1$.*

Demostración. Las dos relaciones son simétricas, así que es suficiente con probar una de ellas, por ejemplo la segunda. La recta L que pasa por P_1 y P_2 corta a la curva elíptica en $-(P_1+P_2)$. Mirando L como la recta que pasa por $-(P_1+P_2)$ y P_2 tenemos que $-(P_1+P_2)+P_2 = -P_1$, que es lo que queríamos.

□

Como el caso en que uno de los puntos $P, Q, R, P+Q$ ó $Q+R$ es ∞ ya ha sido estudiado, vamos a asumir que todos los puntos de la tabla 2.1 son finitos, excepto ∞ y quizás X. Consideremos por separado los siguientes casos:

1. $l_1 = m_1$: Entonces P, Q, R son colineales y, por lo que demostramos anteriormente, la asociatividad se cumple.

2. $l_1 = m_2$: Entonces P, Q y ∞ son colineales, con $P, Q \neq 0$, luego $P+Q = \infty$ y ya demostramos que se cumplía la asociatividad.

3. $l_2 = m_1$: Análogo al anterior.

4. $l_1 = m_3$: Entonces $P, Q, Q+R$ son colineales y por tanto se cumple la asociatividad.

5. $l_3 = m_1$: Análogo al anterior.

6. $l_2 = m_2$: $P+Q$ debe ser $\pm(Q+R)$. Si $P+Q = Q+R$ entonces con la conmutatividad y el Lema 2.3.6, $P = (P+Q)-Q = (Q+R)-Q = R$, y ya demostramos que en este caso se cumplía la asociatividad. Y si $(P+Q) = -(Q+R)$, entonces $(P+Q)+R = -(Q+R)+R = -Q$, y como $P+(Q+R) = P-(P+Q) = -Q$, se cumple la asociatividad.

7. $l_2 = m_3$: En este caso, la recta m_3 que pasa por P y $(Q+R)$ corta a E en ∞ y por tanto $P = -(Q+R)$. Como $-(Q+R), Q, R$ son colineales, por lo que probamos antes, ya tenemos la asociatividad.

8. $l_3 = m_2$: Análogo al anterior.

9. $l_3 = m_3$: Como l_3 no puede cortar a E en 4 puntos (contando multiplicidades), solo puede haber cuatro casos. Que $P = R$ (ya se ha resuelto anteriormente), que $P = P + Q$, que $Q + R = P + Q$ o que $Q + R = R$. Si $P = P + Q$ entonces sumando $-P$ y aplicando el Lema 2.3.6, se tiene que $Q = \infty$ y por tanto se tiene la asociatividad. El caso $Q + R = R$ es similar. En el último caso, si $Q + R = P + Q$, sumando $-Q$ y aplicando el Lema 2.3.6, tenemos que $P = R$, caso que ya hemos visto.

10. $l_i \neq m_j$, con $i, j = 1, 2, 3$: En este caso se cumplen las hipótesis del Teorema 2.3.2 (una la estamos suponiendo y la otra nos la da aplicar el Lema 1.2.26) y por tanto todos los puntos, incluyendo a X, están en E. Sabemos que l_3 corta a E en tres puntos: $R, P+Q, -((P+Q)+R)$ y por descarte $P_{33} = l_3 \cap m_3 = \overline{R, P+Q} \cap \overline{P, Q+R} = -((P + Q) + R)$ y también sabemos que m_3 corta a E en $P, Q + R, -(P + (Q + R))$, e igualmente por descarte $P_{33} = -(P + (Q + R))$. Haciendo la simetría con respecto al eje x, obtenemos que $((P + Q) + R) = (P + (Q + R))$, que es precisamente la asociatividad.

De esta manera, en todos los casos se obtiene que la suma es asociativa y por tanto las curvas elípticas forman un grupo abeliano.

Capítulo 3

El problema del logaritmo discreto

Definición 3.0.7. Sea G un grupo finito. El **Problema del Logaritmo Discreto** es el problema de resolver una ecuación del tipo

$$a^x = b \tag{3.1}$$

con $x \in \mathbb{N}$ y $a, b \in G$.

La dificultad de este problema varía según el grupo G que elijamos. Por ejemplo, si G es $\mathbb{Z}_n$, el problema es resolver una ecuación de congruencias del tipo $ax \equiv b \; mod \; n$, que no es más que resolver la ecuación diofántica $ax + ny = b$ utilizando el Algoritmo de Euclides.
Sin embargo, si G es el grupo de las unidades de $\mathbb{Z}_n$ ó $\mathbb{F}_q$, el problema es considerablemente más difícil.

Sabemos, por la proposición 1.1.12, que $\mathbb{F}_q^*$ es cíclico de orden q-1. Por tanto podríamos pensar que como $\mathbb{F}_q^* \simeq (\mathbb{Z}_{q-1}, +)$, el problema es igual de difícil en ambos. Sin embargo eso solo sería cierto si conociésemos un isomorfismo $f : \mathbb{Z}_{q-1} \longrightarrow \mathbb{F}_q^*$ explícito para el cual pudiésemos calcular tanto $f(x)$ como$f^{-1}(y)$ para $x \in \mathbb{Z}_{q-1}$, $y \in \mathbb{F}_q^*$.

Observemos que la ecuación (3.1) tiene solución si y sólo si b está en el subgrupo cíclico generado por a, luego en la práctica se puede suponer que G es cíclico y por tanto isomorfo a $(\mathbb{Z}_n, +)$, teniendo en cuenta lo dicho en el párrafo anterior. En resumen, la dificultad de este problema no depende de la estructura de G, sino de la forma de presentar los elementos del grupo.

Se ha conjeturado que el problema del logaritmo discreto en un problema $\mathbb{NP}$-completo, pero aún no se ha probado. Sin embargo todos los algoritmos que se conocen para resolver este problema son muy lentos. Así que hoy en día, es irresoluble si se eligen de manera adecuada G y a.

La dificultad de este problema no solo garantiza la seguridad de los sistemas criptográficos de curvas elípticas, sino de otros muchos como Massey-Omura, ElGamal o Blum-Micali, que no veremos y otros como DH ó DSA que los estudiaremos en el siguiente capítulo.

Además de todo esto, el grupo G escogido tiene que tener un algoritmo rápido de cálculo para que los procesos criptográficos sean factibles.

Si queremos calcular x^n, con $x \in G$ y $n \in \mathbb{Z}$, podemos hacerlo de forma rápida utilizando su representación binaria. Si $n = a_0 + 2a_1 + 2^2a_2 + ... + 2^{k-1}a_{k-1}$, tenemos que

$$x^n = x^{a_0+2a_1+2^2a_2+...+2^{k-1}a_{k-1}} = x^{a_0}(x^2)^{a_1}((x^2)^2)^{a_2} \cdots ((x^2)^{n-1})^{a_{k-1}} = x_0^{a_0}x_1^{a_1} \cdots x_{k-1}^{a_{k-1}}.$$

Este algoritmo de exponenciación rápida unido a los rápidos cálculos de las curvas elípticas, hacen que éstas cumplan ese requisito de factibilidad.

En las siguientes secciones veremos algunos de los algoritmos existentes para el cálculo del logaritmo discreto. Algunos son más generales y funcionan en cualquier grupo que tomemos y otros solo sirven para grupos especiales que cumplen alguna condición.

3.1. Fuerza bruta

Es la manera más obvia de resolver este problema. Podemos ir dando valores a x hasta obtener uno que funcione o podemos calcular todas las potencias de a hasta que una nos de b. Claramente este método no es nada eficaz cuando el grupo es muy grande y x puede tomar valores de cientos de dígitos, que es lo que se usa actualmente en criptografía.

3.2. Index-Calculus

Este algoritmo no es general. Solo puede utilizarse en ciertos grupos como los grupos multiplicativos de los cuerpos finitos. Esta pérdida de generalidad se compensa con una mayor eficiencia, ya que saca provecho de las particularidades de estos grupos.

La idea es calcular el logaritmo para varios primos pequeños y usar esa información para calcular el logaritmo para un número aleatorio. Vamos a ver previamente que el logaritmo discreto transforma el producto en suma, igual que ocurre con el logaritmo clásico y después veremos qué hace este algoritmo con un ejemplo.

Sea p primo y g generador del grupo cíclico F_p^*. Entonces todo $h \equiv 0$ (mod p) puede ser escrito de la forma $h \equiv g^k$ para cierto entero k unequívocamente determinado módulo $p-1$. Denotemos $L_g(h)$ el logaritmo discreto de h respecto a g y p, es decir, $L_g(h)$ es un entero (no único) que cumple

$$g^{L_g(h)} \equiv h \ \ (mod \ \ p).$$

Proposición 3.2.1. $L_g(h_1h_2) \equiv L_g(h_1) + L_g(h_2) \ \ (mod \ \ p-1)$.

Demostración. Supongamos que $h = h_1h_2$. Entonces

$$g^{L_g(h_1h_2)} \equiv h_1h_2 \equiv g^{L_g(h_1)+L_g(h_2)} \ \ (mod \ \ p),$$

lo que implica que

$$L_g(h_1h_2) \equiv L_g(h_1) + L_g(h_2) \ \ (mod \ \ p-1).$$

□

Veamos cómo funciona este algoritmo con un ejemplo:

Ejemplo. Sea $n = 1217$ y $a = 3$. Queremos resolver $3^x \equiv 37 (mod\ 1217)$. Primero vamos a hacer un precálculo, independiente del número 37. Vamos a escoger un conjunto B de primos, llamado base de factores, por ejemplo $B = \{2, 3, 5, 7, 11, 13\}$ y vamos a buscar relaciones de la forma

$$3^k \equiv \pm \text{ producto de algunos primos de B (mod 1217)}.$$

Probando con distintos valores de k, encontramos las siguientes:

$$\begin{aligned}
3^1 &\equiv 3 \ \ (mod \ \ 1217)\\
3^{24} &\equiv -2^2 \cdot 7 \cdot 13 \ \ (mod \ \ 1217)\\
3^{25} &\equiv 5^3 \ \ (mod \ \ 1217)\\
3^{30} &\equiv -2 \cdot 5^2 \ \ (mod \ \ 1217)\\
3^{54} &\equiv -5 \cdot 11 \ \ (mod \ \ 1217)\\
3^{87} &\equiv 13 \ \ (mod \ \ 1217)
\end{aligned}$$

Ahora utilizamos la definición de logaritmo y la propiedad que tienen de transformar productos en sumas de la Proposición 3.2.1 para transformar esta congruencias (mod p) en (mod p-1). Por ejemplo:

$$\begin{aligned} 3^{24} &\equiv -2^2 \cdot 7 \cdot 13 \ \ (mod\ \ 1217) \\ 24 &\equiv L_3(-2^2 \cdot 7 \cdot 13) \ \ (mod\ \ 1217) \\ 24 &\equiv L_3(-1) + 2L_3(2) + L_3(7) + L_3(13) \ \ (mod\ \ 1216) \end{aligned}$$

Al ser $\mathbb{F}^*_{1216}$ cíclico, $\mathbb{F}^*_{1216_p} =< g >_n =< 3 >$. Si factorizamos 1216, obtenemos $1216 = 2^6 19$. Como g genera C_n si y solo si $g^{\frac{p}{n}} \neq 1$ para todo $p|n$ con p primo, g^{608} genera un subgrupo de orden dos. Sin embargo, el único subgrupo de orden dos es $< -1 >$, luego $< -1 >_2 =< g^{608} >_2$ y por tanto, como 3 es el generador, $3^{608} \equiv -1$ (mod p), es decir $L_3(-1) = 608$. De esta manera obtenemos:

$$\begin{aligned} 1 &\equiv L_3(3) \ \ (mod\ \ 1216) \\ 24 &\equiv 608 + 2L_3(2) + L_3(7) + L_3(13) \ \ (mod\ \ 1216) \\ 25 &\equiv 3L_3(5) \ \ (mod\ \ 1216) \\ 30 &\equiv 608 + L_3(2) + 2L_3(5) \ \ (mod\ \ 1216) \\ 54 &\equiv 608 + L_3(5) + L_3(11) \ \ (mod\ \ 1216) \\ 87 &\equiv L_3(13) \ \ (mod\ \ 1216) \end{aligned}$$

La primera ecuación nos da que $L_3(3) \equiv 1$ (mod 1216) y aplicando el Algoritmo de Euclides obtenemos de la tercera que $L_3(5) \equiv 819$ (mod 1216) y de la sexta que $L_3(13) \equiv 87$ (mod 1216). De la cuarta obtenemos $L_3(2) \equiv 30 - 608 - 2 \cdot 819 \equiv 216$ (mod 1216), de la quinta que $L_3(11) \equiv 54 - 608 - L_3(5) \equiv 1059$ (mod 1216) y por último, de la segunda, $L_3(7) \equiv 24 - 608 - 2L_3(2) - L_3(13) \equiv 113$ (mod 1216). De esta manera conocemos todos los logaritmos discretos de todos los elementos de la base de factores.

Una vez hecho el preprocesamiento, calculamos $3^j \cdot 37$ (mod p) para varios valores aleatorios de j hasta que obtengamos un entero que pueda ser expresado como producto de primos de B. En nuestro caso, encontramos que

$$3^{16} \cdot 37 \equiv 2^3 \cdot 7 \cdot 11 (mod\ \ 1217).$$

Por tanto,

$$L_3(37) = 3L_3(2) + L_3(7) + L_3(11) - 16 \equiv 588 (mod\ \ 1216),$$

y obtenemos que $3^{588} \equiv 37$ (mod 1217).

Observación. El tamaño de B es importante. Si B es muy pequeño, va a ser difícil encontrar potencias de g que factoricen con primos de B y si B es muy grande, el álgebra necesaria para resolver los logaritmos de B será impracticable.

El tiempo de ejecución esperado de este algoritmo es $exp(\sqrt{2ln(p)ln(ln(p))}$ [31], mucho más rápido (cuando se pueda aplicar) que los que vamos a ver a continuación.

3.3. Baby Step-Giant Step

Este algoritmo no es específico de curvas elípticas sino general, pero nosotros vamos a centrarnos en el logaritmo discreto de las curvas elípticas que es el que nos interesa. Así, dados $P, Q \in G$, queremos resolver $kP = Q$. Vamos a denotar N al órden de G y por simplicidad supondremos que P genera G.

Este algoritmo, desarrollado por D.Shanks requiere aproximadamente $\sqrt{N}$ pasos [31]. Por tanto, solo funciona bien para tamaños moderados de N. El algoritmo es el siguiente:

1. Fijamos un entero $m \geq \sqrt{N}$ y calculamos mP.
2. Calculamos y guardamos los valores iP con $0 \leq i < m$.

3. Calculamos los puntos $Q - jmP$ con $j = 0, 1, ..., m-1$ hasta que uno coincida con alguno de la lista anterior.

4. Si $iP = Q - jmP$, tenemos que $Q = kP$ con $k \equiv i + jm \pmod{N}$.

Este método funciona. Como $m^2 > N$, podríamos asumir que la solución de $kP = Q$, satisface $0 \leq k < m^2$. Tomamos $k = k_0 + mk_1$ con $k_0 \equiv k \pmod{m}$ y $0 \leq k_0 < m$, y $k_1 = (k - k_0)/m$. Entonces $0 \leq k_1 < m$. Cuando $i = k_0$ y $j = k_1$, tenemos que

$$Q - k_1 mP = kP - k_1 mP = k_0 P,$$

luego existe una coincidencia en la lista.

El punto iP se calcula sumando P (un "baby step") a $(i-1)P$. El punto $Q - jmP$ se calcula sumando $-mP$ (un "giant step") a $(Q - (j-1)mP$. De ahí el nombre.

No necesitamos conocer el valor exacto de N, solo una cota superior. Par curvas elípticas sobre F_q podemos usar el Teorema de Hasse 2.1.5 obteniendo que $m^2 \geq q + 1 + 2\sqrt{q}$.

Ejemplo. Sea $G = E(F_{41})$, donde E está dada por $y^2 = x^3 + 2x + 1$. Sean $P = (0, 1)$ y $Q = (30, 40)$. Por el teorema de Hasse 2.1.5, como el orden de G es como mucho 54, tomaremos $m = 8$.

Los puntos iP para $1 \leq i \leq 7$ son:

$$(0, 1), (1, 39), (8, 23), (38, 38), (23, 23), (20, 28), (26, 9).$$

Calculamos $Q - jmP$ para $j = 0, 1, 2$ y obtenemos:

$$(30, 40), (9, 25), (26, 9),$$

punto en el que nos paramos debido a que coincide con $7P$. Como estamos en $j = 2$, tenemos que $(30, 40) = (7 + 2 \cdot 8)P = 23P$, y por tanto $k = 23$.

3.4. Algoritmo ρ de Pollard

Este algoritmo tiene un tiempo de ejecución similar a Baby Step-Giant Step, pero necesita menos memoria.

Sea G un grupo finito de orden N. Elegimos una función $f : G \longrightarrow G$ que se comporte "aleatoriamente"[8, 2]. Comenzamos con un elemento aleatorio P_0 y calculamos iterando, $P_{i+1} = f(P_i)$. Como G es finito, existirán subíndices $i_0 < j_0$ tales que $P_{i_0} = P_{j_0}$, y entonces $P_{i_0+1} = f(P_{i_0}) = f(P_{j_0}) = P_{j_0+1}$, y similarmente $P_{i_0+l} = P_{j_0+l}$ para todo $l \geq 0$. Por tanto la secuencia P_i es periódica con periodo $j_0 - i_0$ (o un posible divisor). La figura 3.1 muestra el proceso, que se parece a la letra griega rho, de ahí el nombre.

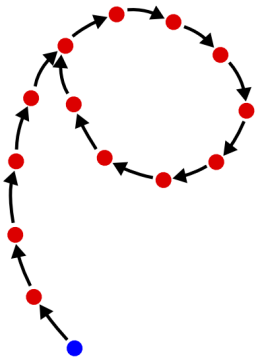

Figura 3.1: Algoritmo Rho. **Fuente**: [19]

Una implementación sencilla sería guardar todos los P_i hasta encontrar una coincidencia, algo que lleva un tiempo del orden de $\sqrt{N}$, igual que el algoritmo anterior. Sin embargo podemos hacerlo mejor. La idea clave es que una vez que hay una coincidencia de dos subíndices que difieren en d, todas las subsecuencias de subíndices que difieran en d van a coincidir también. Esta es precisamente la periodicidad mencionada anteriormente. Por tanto, podemos calcular pares (P_i, P_{2i}) para $i = 1, 2, ...$, pero solo guardar el par actual, no guardamos los anteriores, ya que pueden ser calculados de la siguiente manera:

$$P_{i+1} = f(P_i), \;\; P_{2(i+1)} = f(f(P_{2i})).$$

Supongamos que $i \geq i_0$, i múltiplo de d. Entonces los subíndices i y $2i$ difieren en un múltiplo de d y por tanto $P_i = P_{2i}$. Como $d \leq j_0$ y $i_0 < j_0$, se sigue que hay una coincidencia para $i \leq j_0$. Por tanto el número de pasos para encontrar una coincidencia es como mucho un múltiplo constante de $\sqrt{N}$.

El problema reside en como elegir una función f apropiada. Aparte de que f actúe de manera aleatoria, algo nada trivial, necesitamos ser capaces de extraer información útil de una coincidencia. Vamos a ver como hacerlo para obtener el valor del logaritmo:

1. Dividimos G en s subconjuntos disjuntos $S_1, S_2, ..., S_s$ de aproximadamente igual tamaño.
2. Elegimos $2s$ enteros aleatorios a_i, b_i mod N, $i = 1, .., s$.
3. Tomamos $M_i = a_i P + b_i Q$.
4. Definimos $f(g) = g + M_i$, si $g \in M_i$.

La mejor manera de interpretar f es dar un paseo aleatorio por G, donde los posibles pasos son los elementos M_i.

5. Elegimos enteros aleatorios a_0, b_0 y tomamos $P_0 = a_0 P + b_0 Q$ para que sea el punto de partida del paseo aleatorio.

Mientras calculamos los P_j, anotamos como están expresados en términos de P y Q. Si $P_j = u_j P + v_j Q$ y $P_{j+1} = (u_j + a_i)P + (v_j + b_i)Q$, entonces $(u_{j+1}, v_{j+1}) = (u_j, v_j) + (a_i, b_i)$.

6. Cuando encontramos una coincidencia $P_{j_0} = P_{i_0}$, entonces tenemos que $u_{j_0} P + v_{j_0} Q = u_{i_0} P + v_{i_0} Q$, y por tanto $(u_{i_0} - u_{j_0})P = (v_{j_0} - v_{i_0})Q$.
7. Si $mcd(v_{j_0} - v_{i_0}, N) = d$, tenemos que $k \equiv (v_{j_0} - v_{i_0})^{-1}(u_{i_0} - u_{j_0})$ (mod N/d).

Esto nos da d posibilidades para k. Normalmente d suele ser pequeño, luego podemos probar todas las posibilidades hasta que tengamos $Q = kP$.

Ejemplo. Sea $G = E(F_{1093})$, donde E es la curva elíptica dada por $y^2 = x^3 + x + 1$. Tomaremos $s = 3$, $P = (0, 1)$ y $Q = (413, 959)$. Puede probarse que el orden de P es 1067, pero no es nuestro objetivo ahora mismo. Queremos encontrar k tal que $kP = Q$. Sean $P_0 = 3P+5Q$, $M_0 = 4P+3Q$, $M_1 = 9P + 17Q$, $M_2 = 19P + 6Q$, $f : E(F_{1093}) \longrightarrow E(F_{1093})$ dada por $f(x, y) = (x, y) + M_i$ si $x \equiv i$ (mod 3). Aquí, x es visto como un entero $0 \leq x < 1093$ reducido mod 3, por ejemplo:

$$f(P_0) = P_0 + M_2 = (727, 589),$$

ya que $P_0 = (326, 69)$ y $26 \equiv 2$ (mod 3).

Si encontramos a $f(\infty)$, habremos encontrado una relación de la forma $aP + bQ = \infty$ y podremos obtener k fácilmente.

Si calculamos $P_0, P_1 = f(P_0), P_2 = f(P_1), ...$, obtenemos

$$\begin{aligned} P_0 &= (326, 69), \\ P_1 &= (727, 589), \\ P_2 &= (560, 365), \\ P_3 &= (1070, 260), \\ P_4 &= (47, 903), \\ P_5 &= (1006, 951), \\ P_6 &= (523, 938), \\ &... \\ P_{57} &= (895, 337), \\ P_{58} &= (1006, 951), \\ P_{59} &= (523, 938), \\ &..., \end{aligned}$$

por tanto la secuencia empieza a repetirse en $P_5 = P_{58}$.
Si hacemos el seguimiento de los coeficientes de P y Q en los cálculos, encontramos que

$$P_5 = 88P + 46Q, \quad P_{58} = 685P + 620Q,$$

por tanto,

$$\infty = P_{58} - P_5 = 597P + 574Q.$$

Como P tiene orden 1067, calculamos

$$-574^{-1}597 \equiv 499 \pmod{1067}.$$

De esta manera, $Q = 499P$, y por tanto $k = 499$.

Si en vez de guardar todos los puntos $P_0, P_1, ..., P_{58}$ hasta encontrar una coincidencia, calculamos los pares (P_i, P_{2i}) y solo guardamos el par actual, encontramos que en $i = 53$ está la coincidencia de $P_{53} = P_{106}$. Con esto se obtiene que

$$620P + 557Q = P_{53} = P_{106} = 1217P + 1131Q,$$

y por tanto $597P + 574Q = \infty$ y así $k = 499$, como antes.

3.5. Algoritmo λ de Pollard

Este algoritmo es una generalización del ρ. Al igual que él, hace uso de una función f, pero empieza desde varios puntos aleatorios $P_0^{(1)}, ..., P_0^{(r)}$. De esta manera obtenemos secuencias dadas por:

$$P_{i+1}^{(l)} = f(P_i^{(l)}), \quad 1 \leq l \leq r, \quad i = 0, 1, 2, ...,$$

que pueden ser calculadas por varios ordenadores en paralelo. El objetivo de este algoritmo es hacer que las sucesiones colisionen, ya que cuando se encuentra una coincidencia entre las distintas sucesiones de los ordenadores, tenemos una relación que nos permite resolver el problema del logaritmo discreto de la misma manera que el algoritmo ρ.

Cuando solo hay dos puntos aleatorios inicialmente, tenemos dos paseos aleatorios que con el tiempo tendrán un punto en común, y a partir de él serán iguales. La representación gráfica de este proceso recuerda a la letra griega lambda, de ahí su nombre. Este algoritmo también suele llamarse algoritmo del canguro, haciendo la analogía de que a partir de canguros domados, poniendo trampas, se intenta averiguar desde donde partió el canguro salvaje, la solución a nuestro logaritmo.

Al igual que el algoritmo anterior, se espera encontrar una coincidencia en un tiempo del orden de $\sqrt{N}$, pero si lo paralelizamos, el tiempo puede mejorar significativamente.

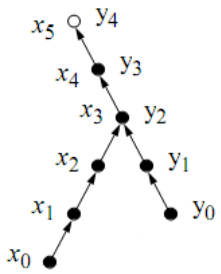

Figura 3.2: Algoritmo Lambda. **Fuente**: [20]

3.6. Algoritmo de Pohlig-Hellman

Como antes, consideramos $P, Q \in G$, y queremos encontrar un entero k tal que $Q = kP$. Conocemos el orden N de P y su factorización en primos:

$$N = \prod_i q_i^{e_i}.$$

La idea de Pohlig-Hellman es encontrar k mod $(q_i^{e_i})$ para cada i, y usar el Teorema Chino de los Restos para combinarlos y obtener k (mod N).

Sea q primo y q^e la potencia exacta de q que divide a N. Escribimos k en base q como

$$k = k_0 + k_1 q + k_2 q^2 + ... + k_{e-1} q^{e-1}$$

con $0 \leq k_i < q$. Vamos a evaluar k mod (q^e) para determinar sucesivamente $k_0, k_1, ..., k_{e-1}$. El procedimiento es el siguiente:

1. Calculamos $T = \left\{ \; j \; \frac{N}{q} \;\; | \;\; 0 \leq j \leq q-1 \right\}$ como conjunto ordenado.
2. Hacemos $r = 0$ y $Q_r = Q_0 = Q$.
3. Mientras que $r < e$:
   - *a*) Calculamos $\frac{N}{q^{r+1}} Q_r$ que ha de ser un elemento de T. Calculamos k_r de forma que $\frac{N}{q} Q_r$ sea el elemento $k_r + 1$ de la lista T.
   - *b*) Hacemos $Q_{r+1} = Q_r - k_r q^r P$.
   - *c*) $r = r + 1$.

De esta manera tenemos

$$k \equiv k_0 + k_1 q + ... + k_{e-1} q^{e-1} \;\; (mod \;\; q^e).$$

¿Por qué funciona? Supongamos que $(k'_0, k'_1, ..., k'_{e-1})$ es la salida del algoritmo. Tenemos que demostrar que $k_i = k'_i$ para todo $i = 1, ..., e-1$.
Supongamos que ya sabemos que $k_j = k'_j$ para todo $j < i$. Entonces

$$\frac{N}{q^{r+1}} Q_r = k'_i \frac{N}{q} P$$

y

$$Q_{r+1} = Q_r - k'_r q^r P.$$

Por tanto

$$Q_{r+1} = Q - (k'_0 + k'_1 q + ... + k'_r q^r) P = [(k_0 - k'_0) + (k_1 - k'_1) q + ... + (k_r - k'_r) q^r + k_{r+1} q^{r+1} + ... + k_{e-1} q^{e-1}] P.$$

Como $k_j = k'_j$ para todo $j < i$,

$$Q_i = (k_i q^i + ... + k_{e-1} q^{e-1})P$$

y entonces

$$k'_i \frac{N}{q} P = \frac{N}{q^{i+1}} Q_i = k_i \frac{N}{q} P.$$

Y como $\frac{N}{q}P$ tiene orden q y $0 \leq k_i, k'_i < q$, necesariamente $k_i = k'_i$.

Ejemplo. Sea $G = E(F_{599})$, donde E es la curva elíptica dada por $y^2 = x^3 + 1$. Sean $P = (60, 19), Q = (277, 239)$. Puede probarse que el orden de P es $N = 600$, pero no es el objetivo de este ejemplo. Queremos resolver $Q = kP$ para algún k. La factorización en primos de N es $600 = 2^3 \cdot 3 \cdot 5^2$.

Vamos a calcular k mod 8, mod 3 y mod 25, para después combinarlos y obtener k mod 600 (el teorema chino de los restos nos permite hacerlo).

- **k mod 8**: Tenemos que $T = \{\infty, (598, 0)\}$. Como

  $$\frac{N}{2}Q = \infty = 0 \cdot (\frac{N}{2}P),$$

  tenemos que $k_0 = 0$ y que $Q_1 = Q - 0P = Q$.

  Como

  $$(\frac{N}{4})Q_1 = 150Q_1 = (598, 0) = 1 \cdot \frac{N}{2}P,$$

  tenemos que $k_1 = 1$, y por tanto $Q_2 = Q_1 - 1 \cdot 2 \cdot P = (35, 243)$.

  Como

  $$(\frac{N}{8})Q_2 = 75Q_2 = \infty = 0 \cdot \frac{N}{2}P,$$

  tenemos que $k_2 = 0$, y por tanto $k = 0 + 1 \cdot 2 + 0 \cdot 4 + ... \equiv 2 \pmod 8$.

- **k mod 3**: Tenemos que $T = \{\infty, (0, 1), (0, 598)\}$. Como

  $$\frac{N}{3}Q = (0, 598) = 2 \cdot \frac{N}{3}P,$$

  tenemos que $k_0 = 2$ y por tanto $k \equiv 2 \pmod 3$.

- **k mod 25**: Tenemos que $T = \{\infty, (84, 179), (491, 134), (491, 465), (84, 420)\}$. Como

  $$\frac{N}{5}Q = (84, 179)$$

  tenemos que $k_0 = 1$ y por tanto $Q_1 = Q - 1 \cdot P = (130, 129)$.

  Como

  $$(\frac{N}{25})Q_1 = (491, 465),$$

  tenemos que $k_1 = 3$, y por tanto $k = 1 + 3 \cdot 5 + ... \equiv 16 \pmod{25}$.

De esta manera tenemos las congruencias

$$\begin{cases} x \equiv 2 \pmod 8, \\ x \equiv 2 \pmod 3, \\ x \equiv 16 \pmod{25}. \end{cases}$$

Combinándolas, obtenemos $k \equiv 266 \pmod{600}$, luego $k = 266$.

Este método funciona bien si todos los primos que dividen a N son pequeños, ya que si q es un primo grande, T contendrá q elementos.

Capítulo 4

Criptografía con curvas elípticas

La criptografía se suele dividir en criptografía **simétrica** y **asimétrica**. Los algoritmos simétricos se caracterizan por el uso de una misma clave para cifrar y descifrar. Obviamente ambas partes (emisor y receptor) deben conocer la clave de antemano y si la llave llega a manos de terceros, el sistema dejaría de ser seguro. Por contra, los algoritmos asimétricos disponen de dos claves, una pública que se utiliza para cifrar y que está disponible para cualquiera que desee utilizarla y otra privada que se utiliza para descifrar. En la figura 4.1 se puede ver una clasificación de los algoritmos más conocidos en función de su objetivo criptográfico y del tipo de criptografía empleada. En este trabajo vamos a centrarnos en los algoritmos asimétricos, en particular los de curvas elípticas.

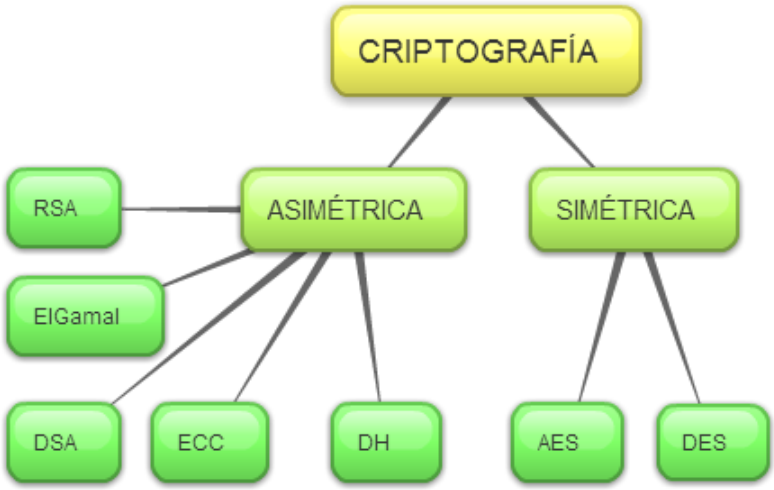

Figura 4.1: Taxonomía no exhaustiva de la criptografía

Los algoritmos simétricos son más eficientes, pues las operaciones aritmético lógicas llevadas a cabo son de ejecución rápida en ordenadores (desplazamiento de bits, AND, OR, XOR...). Además, sólo se necesita una clave y no necesitan de ningún tercero que certifique que una clave pública pertenece a una cierta entidad fiable. El problema viene cuando queremos establecer la clave común, que es lo que se conoce como distribución de claves simétricas. No podemos mandarla sin cifrar porque cualquier persona la podría ver y no habría servido para nada. Tampoco podemos asegurar quién es el autor de un mensaje, ya que ambos extremos comparten la clave. Este problema es el que resuelven los algoritmos asimétricos, que normalmente no se utilizan para cifrar mensajes debido a que su coste es más alto (la clave es más grande y las operaciones matemáticas involucradas son más costosas), sino que se emplean para establecer la clave simétrica de manera segura. Estos algoritmos garantizan el resto de propiedades criptográficas que los algoritmos simétricos no pueden garantizar, como el no repudio.

Las operaciones criptográficas que nos van a interesar especialmente son las de cifrado y descifrado, intercambio de claves simétricas y firma digital (así como la verificación de dicha firma). Veamos en que consisten cada uno de ellas para más tarde centrarnos en las particularidades de cada algoritmo.

4.1. Operaciones criptográficas generales

4.1.1. Cifrado y descifrado

En criptografía asimétrica, para cifrar un mensaje (confidencialidad), como hemos dicho anteriormente, se utiliza la clave pública del individuo al que queremos enviar dicho mensaje. La información sólo podrá descifrarse con la clave privada propia. El proceso puede verse de forma esquemática en la figura 4.2.

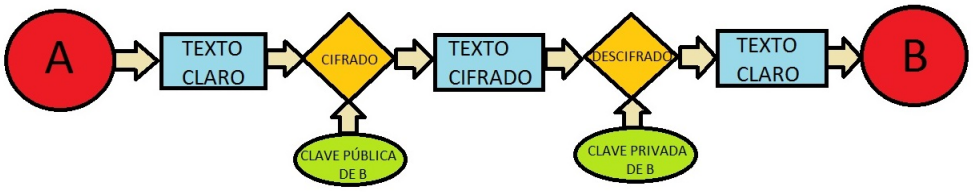

Figura 4.2: Cifrado y descifrado asimétrico

4.1.2. Intercambio de claves simétricas

Uno de los propósitos de la criptografía asimétrica es intercambiar claves simétricas. El intercambio de claves simétricas (o key agreement) se utiliza para obtener la clave con la que posteriormente cifraremos los mensajes usando un algoritmo simétrico, debido a que la criptografía simétrica es más eficiente (sus operaciones son más sencillas y, por tanto, más rápidas). Como aún no se ha establecido una clave, la información viaja por un canal inseguro y hacia un receptor aún no autenticado. Por tanto, cualquier persona podría estar escuchando la conversación o haciéndose pasar por el receptor. La labor de este intercambio de claves es precisamente crear un canal seguro y garantizar que aunque alguien esté escuchando, no pueda obtener la clave simétrica intercambiada con la información que roba. Veremos como se consigue analizando más tarde el algoritmo Diffie-Hellman (DH) en su versión original y en su versión con curvas elípticas.

4.1.3. Firma y verificación

Esta operación es muy importante, puesto que garantiza la autenticación, el no repudio y la integridad en una comunicación.

El modelo más implementado de firma consiste en hacer un "resumen" del mensaje mediante una función hash, por ejemplo SHA-1[36]. Esta función transforma el mensaje en un bloque de longitud fija. Posteriormente, este resumen se cifra con la clave privada propia (esto es lo que se denomina firma) y se adjunta al mensaje original. En la figura 4.3 se puede ver este proceso.

Lo interesante de la firma radica en la verificación que es donde se comprueba que realmente la firma es válida y se garantizan las propiedades que queríamos de autenticación, integridad y no-repudio. Para ello, cuando nos llega un mensaje firmado y lo desciframos, lo primero que se hace es utilizar la función hash para generar el resumen del texto original. Así disponemos del resumen cifrado con la clave privada del emisor y del resumen en claro. Sólo tenemos que utilizar la clave pública del emisor para descifrar el resumen encriptado y comprobar si los resúmenes coinciden, en cuyo caso, el mensaje no ha sido alterado y se garantiza la integridad. Además, el que el emisor utilice su propia clave privada para cifrar el resumen, garantiza el no repudio y la autenticación, puesto que sólo su clave pública puede descifrar la información. Si no se pudiese descifrar, podemos concluir que el emisor no es quien dice ser.

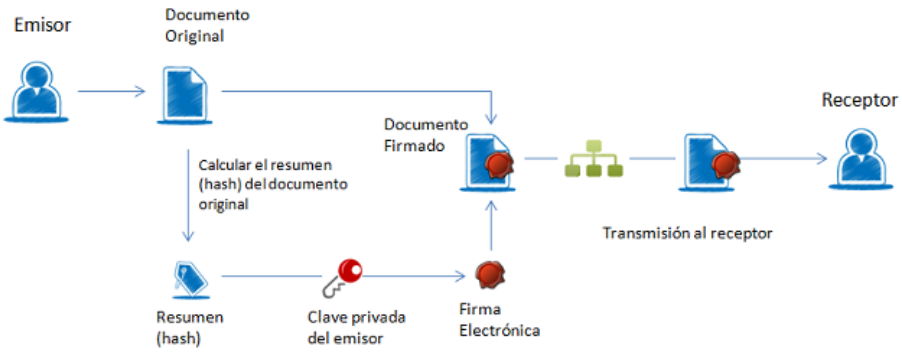

Figura 4.3: Firma. **Fuente**: [17]

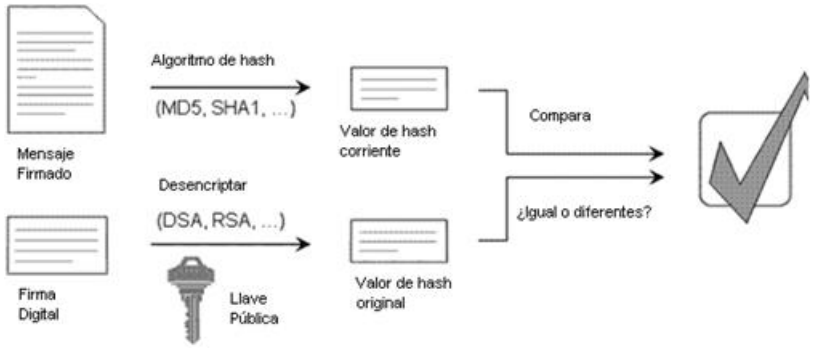

Figura 4.4: Verificación de la firma. **Fuente**: [18]

Una vez conocidas estas operaciones básicas, para poder adentrarnos en el mundo de las curvas elípticas necesitamos conocer unas nociones básicas de los algoritmos de criptografía asimétrica más conocidos y utilizados, que constituyen la base de los algoritmos con curvas elípticas. Nos referimos a RSA, DSA y DH.

4.2. RSA

Este algoritmo fue ideado en 1977 por Ron Rivest, Adi Shamir y Leonard Adleman (las letras RSA son las iniciales de sus apellidos). Es el más empleado en la actualidad, sencillo de comprender e implementar, aunque la longitud de sus claves es bastante considerable, ya que ha pasado desde sus 200 bits originales a los 2048 bits que se usan actualmente. RSA es la suma de dos de los algoritmos más importantes de la historia: el Máximo Común Divisor de Euclídes (Grecia, 450-377 A.C.) y el Pequeño Teorema de Fermat[1] (Francia, 1601-1665).

Su seguridad se basa en la dificultad de factorizar números primos de gran tamaño, ya que aunque en principio, se puede deducir la clave secreta conociendo la clave pública, solo podría hacerse por medio de la factorización de números de gran longitud (centenares de cifras), lo que hace el problema intratable.

Cada participante genera las claves necesarias que se utilizarán para cifrar y descifrar siguiendo el siguiente procedimiento:

- Elegimos dos números primos aleatorios, p y q de la misma longitud. Esto puede hacerse mediante un test de primalidad, es decir, eligiendo números al azar, y viendo si son primos hasta que lo consigamos.

[1]Puede encontrarse el enunciado y la demostración en la bibliografía [5].

- Se calcula $n = pq$ y n se usa como el módulo de las claves pública y privada. Actualmente[3] el tamaño de n es de al menos 1024 bits, aunque se recomienda ya el uso de 2048 bits, y se prevé que siga creciendo con la capacidad de cálculo de los ordenadores.
- Se calcula la función de Euler: $\varphi(n) = (p-1)(q-1)$, también llamada "indicatriz", y que, para un número entero n es igual al número de enteros positivos menores o iguales a n y que son coprimos con él. Esta función cumple que si $mcd(u, v) = 1$, entonces $u^{\varphi(v)} \equiv 1 \ mod \ v$. Esto motiva el siguiente paso.
- Se elige un entero positivo e coprimo con $\varphi(n)$. Esta e se utiliza como el exponente de la clave pública.
- Se calcula d tal que $d \equiv e^{-1} \ mod \ \varphi(n)$, lo que suele hacerse mediante el algoritmo[15] de euclides extendido. El número d se utiliza como el exponente de la clave privada.

De esta manera, tenemos que la clave pública es el par (n, e) y la privada el par (n, d).

Para cifrar y descifrar un mensaje se utiliza el mismo esquema que mencionamos en el apartado anterior y que aparece en la figura 4.2, pero con las claves propias de RSA y algunas particularidades más:

- Primero, se divide el mensaje en bloques de tamaño entero menor que n y si es necesario, se utiliza una función de padding, es decir una función que "rellena" el mensaje, en este caso añadiendo ceros por la izquierda, para que la longitud del mensaje no ponga en jaque a la seguridad del cifrado.
- Una vez que hemos dividido el mensaje en bloques, se cifra cada bloque haciendo $c \equiv m^e \ mod \ n$.
- Se envían los bloques cifrados c.
- Cuando el receptor recibe los bloques, los descifra haciendo $m \equiv c^d \ mod$.
- Se deshace el padding y obtenemos el mensaje original.

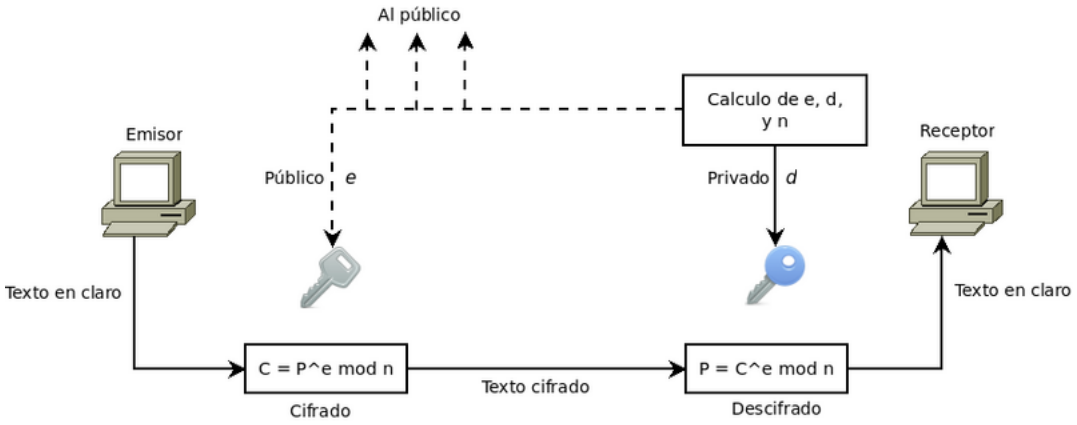

Figura 4.5: Cifrado y descifrado con RSA. **Fuente**: [32]

Observación. Cuando ciframos con exponentes pequeños y valores pequeños de m, el resultado de m podría ser estrictamente menor que el módulo de n. En este caso, el texto cifrado podría ser fácilmente descifrado, tomando la raíz e-ésima del texto cifrado sin tener en cuenta el módulo. Un mensaje que fuese un solo carácter ASCII NULL (cuyo valor es 0) se codificaría como m=0, produciendo un texto cifrado de 0 sin importar qué valores de e y N son usados.

Además, RSA es un algoritmo determinista (no tiene componentes aleatorias) luego un atacante puede ir construyendo un diccionario de textos probables con la clave pública, y almacenando el resultado cifrado. Observando los textos cifrados en un canal de comunicación, el

atacante puede usar este diccionario para descifrar el contenido del mensaje. El padding asegura que m no caerá en el rango de textos sin cifrar inseguros, y que dado un mensaje, una vez que este rellenado se cifrará, por lo que se incrementaría el diccionario haciendo intratable realizar ese ataque. Por eso la necesidad del padding. Las funciones de padding son invertibles, luego se puede recuperar el mensaje original disponiendo del mensaje rellenado.

4.3. DH

El algoritmo de Diffie-Hellman fue publicado en 1976 por Whitfield Diffie y Martin Hellman. Este algoritmo permite acordar una clave secreta entre dos máquinas, a través de un canal inseguro y enviando únicamente dos mensajes. La clave secreta resultante no puede ser descubierta por un atacante, aunque éste obtenga los dos mensajes enviados por el protocolo. La principal aplicación de este protocolo es acordar una clave simétrica con la que posteriormente cifrar las comunicaciones entre dos máquinas. Actualmente se conoce que es vulnerable a ataques de middle-in-the-man (MitM): un atacante podría situarse entre ambas máquinas y acordar una clave simétrica con cada una de las partes, haciéndose pasar por el individuo A de cara al B y viceversa. Una vez establecidas las 2 claves simétricas, el atacante haría de puente entre los dos, descifrando toda la comunicación y volviéndola a cifrar para enviársela al receptor legítimo. Para corregir la vulnerabilidad del protocolo, éste debe ser utilizado conjuntamente con algún sistema que autentique los mensajes. Nosotros lo veremos posteriormente utilizado junto con las curvas elípticas. Veamos como se intercambian las claves:

- Tanto el emisor (A) como el receptor (B) acuerdan un primo n y g un generador de $\mathbb{Z}_p^*$.
- A escoge un número aleatorio x y envía $X = g^x \ mod \ n$.
- B escoge un número aleatorio y y envía $Y = g^y \ mod \ n$.
- A calcula $k = Y^x \ mod \ n$.
- B calcula $k' = X^y \ mod \ n$.
- Finalmente se tiene que $k = k' = g^{xy} \ mod \ n$, siendo k el secreto compartido.

Las condiciones para que este algoritmo funcione son que n sea suficientemente grande y que $(n-1)/2$ sea primo. La validez del secreto k depende de la intratabilidad del logaritmo discreto para n grande, luego conociendo g, n, X e Y es muy costoso calcular k. El problema del logaritmo discreto es también la base de los algoritmos de curva elíptica.

Observación. A pesar de que DH utilice el grupo $\mathbb{Z}_p^*$, este algoritmo se puede trasladar a cualquier otro.

4.4. DSA

El algoritmo de firma digital (DSA, Digital Signature Algorithm) es un estándar del Gobierno Federal de los Estados Unidos de América o FIPS para firmas digitales desde 1993. Lo propuso el National Institute of Standards and Technology (NIST) en 1991. Con el certificado DSA es más fácil estar al día en cuanto a normas gubernamentales, ya que lo respaldan las agencias federales (incluyendo el cambio obligatorio a las claves de 2048 bits). Este algoritmo (como su nombre lo indica) sirve para firmar y no para cifrar información.

El funcionamiento de DSA se divide en 3 etapas[2]. Generación de claves, firma y verificación. Las dos primeras las realiza el emisor y la última el receptor.

1. Generación de claves
    - Elegimos p primo de L bits, donde $512 \leq L \leq 1024$ y L es divisible por 64.

[2]Puede encontrarse la demostración del buen funcionamiento de este algoritmo en [34]

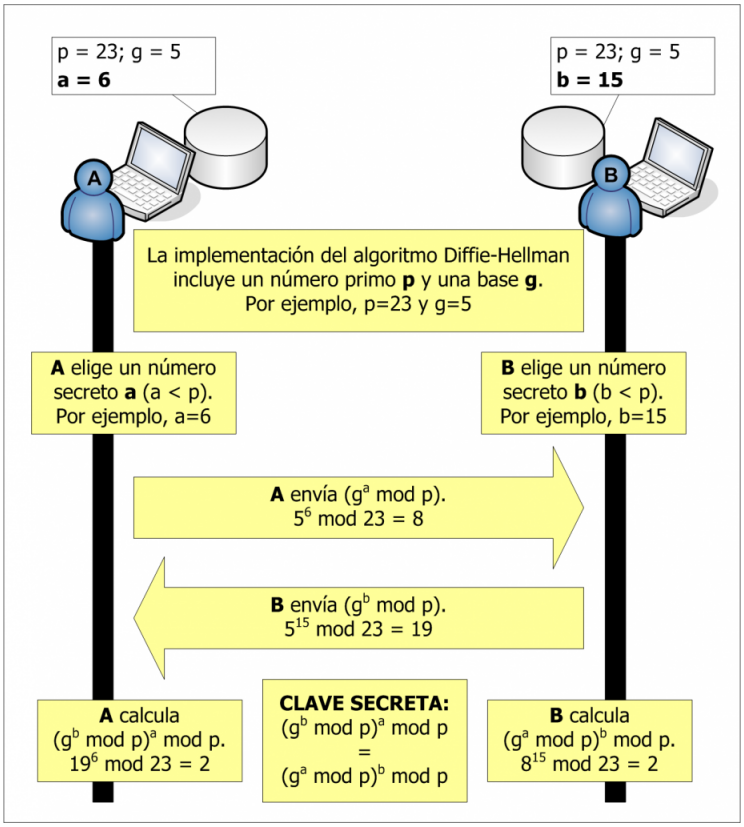

Figura 4.6: Ejemplo básico de intercambio DH. **Fuente**: [4]

- Elegimos un número primo q de 160 bits, tal que $p - 1 = qz$, con $z \in \mathbb{N}$.
- Elegimos h, donde $1 < h < p - 1$ tal que $g = h^z \ mod \ p > 1$.
- Elegimos x de forma aleatoria, donde $1 < x < q - 1$.
- Calculamos $y = g^x \ mod \ p$.
- Finalmente tenemos que p, q, g e y son públicos y x es la clave privada.

2. Firma

- Elegimos un número aleatorio k, donde $1 < k < q$
- Calculamos $r = (g^k \ mod \ p) \ mod \ q$.
- Calculamos $s = k^{-1}(H(m) + rx) \ mod \ q$, donde $H(m)$ es la función hash SHA-1 aplicada al mensaje m.
- De esta forma tenemos que la firma es el par (r, s).
- Nota: Si r ó s es cero, se vuelve a repetir el procedimiento.

3. Verificación

- Calculamos $w = s^{-1} \ (mod \ q)$.
- Calculamos $u_1 = H(m)w \ (mod \ q)$.
- Calculamos $u_2 = rw \ (mod \ q)$.
- Calculamos $v = [g^{u_1} y^{u_2} \ mod \ p] \ mod \ q$.
- De esta manera la firma es válida si $r = v$.

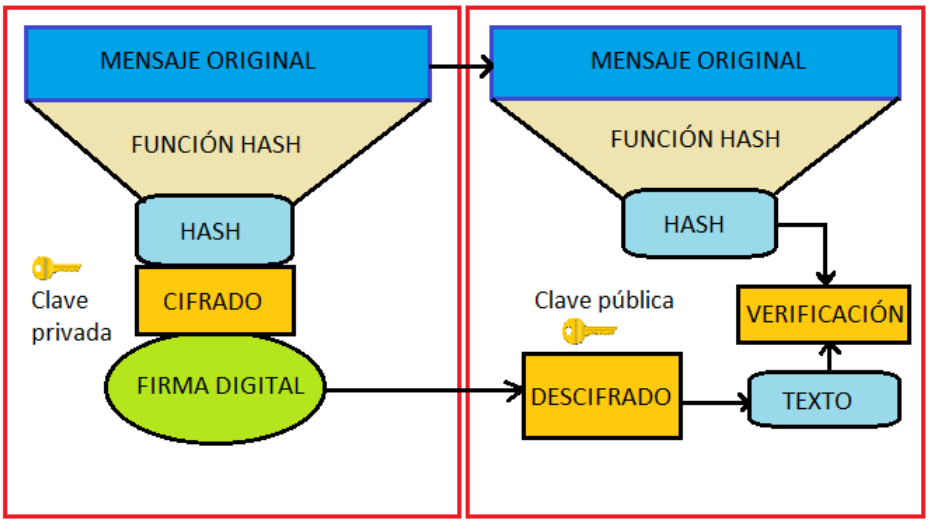

Figura 4.7: DSA

4.5. AES

AES (Advanced Encryption Standard) también conocido como Rijndael, es un esquema de cifrado por bloques adoptado en el año 2003 como un estándar de cifrado por el gobierno de los Estados Unido. El cifrado fue desarrollado por dos criptólogos belgas, Joan Daemen y Vincent Rijmen, ambos estudiantes de la Katholieke Universiteit Leuven, y enviado al proceso de selección AES bajo el nombre Rijndael". Trabaja con bloques de 128 bits y con claves de 128, 192 y 256 bits. Dependiendo del tamaño de la clave, el número de rondas va desde 10 hasta 14. Este algoritmo considera ciclos con cuatro transformaciones matemáticas: ByteSub (sustitución de bytes), ShiftRow (desplazamiento de filas), MixColumns (multiplicación de columnas), y AddRoundKey (se aplica un or-exclusivo entre los bits del texto y la llave). En el último ciclo sólo se ejecutan las siguientes transformaciones: ByteSub, ShiftRow y AddRoundKey.

4.6. ECC

Los criptosistemas de curva elíptica (ECC) fueron inventados por Neal Koblitz y Victor Miller in 1985. En las siguientes secciones veremos como se realizan las principales operaciones criptográficas utilizando las operaciones sobre el grupo de las curvas elípticas.

4.6.1. Generación de claves

- Se establece un primo p y una curva elíptica $y^2 = x^3 + ax + b$ sobre $\mathbb{Z}_p$.
- Se establece un elemento G de la curva, de orden primo q de longitud similar a p.
- Se elige aleatoriamente un entero $d \in [0, q-1]$ y se calcula $P = dG$.
- La clave pública es P y los valores (a, b, q, G) son todos públicos.
- La clave privada es d.

En la tabla 4.1 pueden verse los valores actuales usuales para las claves pública y privada.

Observación. Nótese que sobre el entero d no hay más restricción que el rango [0,q-1], al contrario que en RSA, que debía de ser primo. Este es principalmente el motivo por el cual la generación de claves es más rápida en curvas elípticas.

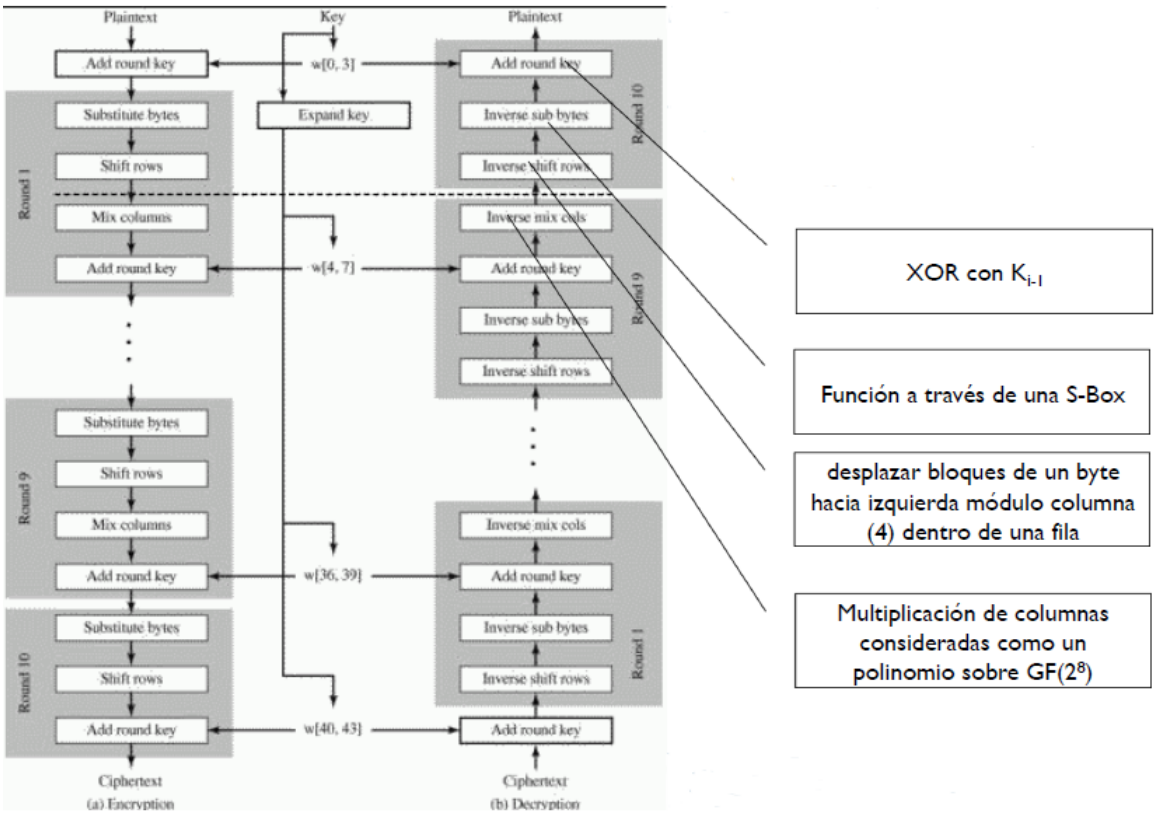

Figura 4.8: Cifrado simétrico con AES. **Fuente**: [13]

4.6.2. Intercambio de claves (ECDH)

Elliptic curve Diffie–Hellman (ECDH) es un protocolo de intercambio de claves que permite a dos individuos que disponen de una clave pública y otra privada, establecer un secreto compartido. Este secreto puede ser directamente usado como clave o para derivar una clave. En particular, es una variante del protocolo Diffie–Hellman (DH) usando curvas elípticas.

Veamos los pasos para obtener ese secreto compartido:

- Tanto el emisor) como el receptor B acuerdan una curva elíptica E sobre un cuerpo finito Z_p suficientemente segura y acuerdan un punto $G \in E(Z_p)$ tal que el subgrupo generado por G sea de un orden grande.
- A elige un entero aleatorio a y envía $P_A = aG$.
- B elige un entero aleatorio b y envía $P_B = bG$.
- A calcula $aP_B = abG$.

Protocolo	Clave pública (bits)	Clave privada (bits)
RSA	1088	2048
DSA	1024	160
ECC	161	160

Tabla 4.1: Tamaños de claves públicas y privadas

- B calcula $bP_A = abG$.
- Finalmente se tiene que la coordenada x de abG es el secreto compartido.

Observación. La seguridad de este secreto radica en la dificultad de resolver el problema del logaritmo discreto, es decir, conociendo G, aG y $bG \in E(Z_p)$, calcular abG. Para ello, p debe ser suficientemente grande.

4.6.3. Cifrado y descifrado

Para cifrar, se puede utilizar el secreto compartido que obtenemos con DH, usándolo como clave o aplicándole una función KDF[3] (key derivation function) que deriva una o varias claves a partir del secreto compartido. Esta clave simétrica entonces se puede utilizar con un algoritmo simétrico como AES[28].

También podemos utilizar criptografía asimétrica, en particular curvas elípticas, para cifrar nuestro mensaje, utilizando algoritmos como ElGamal o Massey-Omura adaptados a ellas.

Nosotros nos centraremos en ECIES (Elliptic curve integration scheme), un esquema de cifrado híbrido que utiliza las claves públicas y privadas y el cifrado simétrico.

ECIES

ECIES fue creado por Bellare y Rogaway y propuesto como estándar por Victor Shoup en el año 2001. ECIES combina un mecanismo de encapsulación de la clave (KEM) con un mecanismo de encapsulación de los datos (DEM). El sistema saca por separado una clave para cifrar y una clave MAC a partir de un secreto compartido. Primero, los datos se encriptan simétricamente, y después el texto cifrado se autentica con el MAC. Por último, el secreto común se encripta usando el par de claves pública/privada. La salida de la función de cifrado es la tupla $\{K, C, T\}$, donde K es el secreto compartido cifrado, C es el texto cifrado y T es la etiqueta de autenticación.

Por tanto, ECIES necesita dos funciones hash H_1, H_2 y una función de cifrado simétrico E_k (dependiente de la clave k). Una vez que se han establecido las claves públicas y privadas de los participantes, si A quiere mandar un mensaje a B, tendrá que hacer:

- A elige un entero aleatorio k, $1 \leq k \leq N-1$, donde N es el orden del punto G que mencionamos en el apartado 4.6.1.
- A calcula $R = kG$ y $Z = kK_{pubB}$.
- A escribe la salida de $H_1(R, Z)$ como dos cadenas k_1, k_2 concatenadas de longitudes específicas.
- A calcula $C = E_{k_1}(m)$ y $t = H_2(C, k_2)$.
- A envía el texto cifrado (R, C, t) a B.

Y para descifrar, B deberá hacer:

- B calcula $Z = K_{privB}R$.
- B calcula $H_1(R, Z)$ y escribe la salida como $k_1||k_2$.
- B calcula $H_2(C, k_2)$. Si no es igual a t, B para y rechaza el descifrado. Y si es igual a t, continúa.
- B calcula $m = D_{k_1}(C)$, donde D_{k_1} es la función de descifrado para E_{k_1}.

[3]Más información en `http://en.wikipedia.org/wiki/Key_derivation_function`

Observación. Un paso importante es el procedimiento de autenticación del paso 3. En muchos criptosistemas, un atacante puede elegir varios textos cifrados y mandárselos a B para que los descifre. Estas desencriptaciones pueden utilizarse para atacar el sistema. En este algoritmo, el atacante puede generar textos cifrados eligiendo C y k_2' y obteniendo $t' = H_2(C, k_2')$. Sin embargo el atacante no conoce el valor de Z, luego no puede usar el mismo valor k_2 que B obtiene de $H_1(R, Z)$. Es muy improbable que $t' = t$. Así que con una alta probabilidad, B simplemente rechazará la operación de descifrado y se evitará el ataque.

ElGamal

Veamos como un caso representativo de la otra opción para cifrar con curvas elípticas, el algoritmo de ElGamal.

Para cifrar realizamos los siguientes pasos:

- A elige un entero aleatorio k y calcula $C_1 = kG$, $C_2 = kK_{pubB}$.
- A utiliza una función que pase el mensaje a un punto de la curva. Esta función debe tener inversa. Así, tenemos $M = f(m)$, donde m es el texto en claro.
- A envía el texto cifrado $(C_1, C_2 + M)$.

Para que B descifre el mensaje, es necesario que haga:

- B recibe el texto cifrado (M_1, M_2).
- B calcula $M = M_2 - K_{privB}M_1$.
- B utiliza la inversa de la función que transforma el mensaje en un punto de la curva para obtener el texto en claro m.

Observación. Este proceso funciona, ya que $M_2 - K_{privB}M_1 = (C_2 + M) - K_{privB}kG = M + kK_{pubB} - K_{privB}kG = M + k(K_{privB}G) - K_{privB}kG = M$

Observación. Una ventaja de ECIES sobre Massey-Omura y ElGamal es que los mensajes no tienen que representarse como puntos de la curva, por tanto nos ahorramos el tiempo de transformar el mensaje en dichos puntos[10].

4.6.4. Firma y verificación (ECDSA)

Elliptic Curve Digital Signature Algorithm (ECDSA) es una modificación del algoritmo DSA que emplea operaciones sobre puntos de curvas elípticas en lugar de las exponenciaciones que usa DSA (problema del logaritmo discreto). Fue aceptado en el año 1999 como estándar ANSI y en el año 2000 como estándar en IEEE y NIST. En el 1998 también fue aceptado como estándar ISO y actualmente está pendiente de incluirse en otros estándares ISO.

Veamos como A puede generar una firma con ECDSA:

- A selecciona un entero aleatorio k, $1 \leq k \leq N - 1$, donde N es el orden del elemento G que mencionamos en el apartado 4.6.1 y calcula $kG = (x_1, y_1)$.
- A trata a x_1 como un entero y calcula $r = x_1 \ mod \ n$. Si $r = 0$, vuelve al primer paso.
- A calcula $k^{-1} \ mod \ n$.
- A calcula $e = H(m)$, donde H es una función hash como por ejemplo SHA-1, y lo pasa a entero.
- A calcula $s = k^{-1}(e + K_{privA}r) \ mod \ n$. Si $s = 0$, vuelve al primer paso.
- Finalmente, la firma del mensaje m es (r, s).

Y para que B pueda verificar la firma de A:

- B verifica que $r, s \in [1, N-1]$.
- B calcula $e = H(m)$, donde H es una función hash utilizada en la firma, y lo pasa a entero.
- B calcula $w = s^{-1} \ mod \ n$.
- B calcula $u_1 = ew \ mod \ n$ y $u_2 = rw \ mod \ n$.
- B calcula $X = u_1 G + u_2 K_{pubA} = (x_1, y_1)$.
- Si X es el punto del infinito de la curva, se rechaza la firma. Si no, B trata a x_1 como un entero y calcula $v = x_1 \ mod \ n$.
- Finalmente, la firma se acepta si, y solo si $r = v$.

Observación. Este proceso funciona, ya que

$$k \equiv s^{-1}(e + K_{privA} r) \equiv s^{-1}e + s^{-1} r K_{privA} \equiv we + wrK_{privA} \equiv u_1 + u_2 K_{privA} \ \ mod \ \ n$$

. Por tanto,

$$u_1 G + u_2 K_{pubA} = (u_1 + u_2 d)G = kG$$

y entonces $v = r$, como queríamos ver.

Bibliografía

[1] ÁNGEL ÁNGEL, J.J. *Criptografía Para Principiantes.* <http://www.math.com.mx/criptografia.html> [Consulta: 4 de abril de 2015]

[2] AZOR MONTOYA, J.R. *Funciones aleatorias.* Mendoza: Universidad de Mendoza (Argentina). <http://www.um.edu.ar/math/mariana/2-estocas.pdf> [Consulta: 30 de mayo de 2015]

[3] BONEH, D. (1999) "Twenty Years of Attacks on the RSA Cryptosystem" en American Mathematical Society (AMS), Vol. 46, No. 2, p. 203-213. <http://crypto.stanford.edu/~dabo/pubs/papers/RSA-survey.pdf> [Consulta: 4 de abril de 2015]

[4] CAMPOS, J. (2011) *El algoritmo de Diffie-Hellman.* <http://www.javiercampos.es/blog/2011/07/22/el-algoritmo-de-diffie-hellman/> [Consulta: 16 de junio de 2015]

[5] CHAN, H.L. y NORRISH, M.(2013) "Proofs of Fermat's Little Theorem" en Journal of Formal Reasoning, Vol 6, No. 1, p. 63-87. <http://jfr.unibo.it/article/view/3728> [Consulta: 30 de mayo de 2015]

[6] FIPS (2013). *Digital Signature Standard (DSS).* FIPS 186. Gaithersburg,: FIPS. <https://oag.ca.gov/sites/all/files/agweb/pdfs/erds1/fips_pub_07_2013.pdf>

[7] GELCA, R. (2014). "Un problema de geometría combinatoria y las curvas elípticas" en Universo.math, Vol 1,Núm 3, Artículo 5. <http://universo.math.org.mx/2014-3/olimpiada/un-problema-de-geometria.html> [Consulta: 15 de junio de 2015]

[8] GOLDREICH, O., GOLDWASSER, S. y MICALI, S. (1986) *How to construct random functions.* Massachusetts: Instituto tecnológico de Massachusetts. <http://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Pseudo%20Randomness/How%20To%20Construct%20Random%20Functions.pdf>. [Consulta: 30 de mayo de 2015]

[9] HOLME, A. (2010). *Geometry: Our Cultural Heritage*, p. 321-323.

[10] HUGUET, L., RIFÀ, J. y TENA, J.G. *Criptografía con curvas elípticas.* Cataluña: Universidad abierta de Cataluña. p. 41-46,55-59. <http://www.exabyteinformatica.com/uoc/Informatica/Criptografia_avanzada/Criptografia_avanzada_(Modulo_4).pdf> [Consulta: 25 de mayo de 2015]

[11] KNAPP, A. W. (1992). *Elliptic Curves*, p. 38-44,75-76.

[12] LUNA, C. y MORRILLO, P. (2009) *Aplicaciones de las curvas elípticas a la criptografía.* <http://divulgamat2.ehu.es/divulgamat15/index.php?option=com_content&task=view&id=9874&Itemid=67&showall=1> [Consulta: 13 de abril de 2015]

[13] MARÍN LÓPEZ, R.(2013). *Servicios Telemáticos.* Murcia: Universidad de Murcia, Facultad de Informática.

[14] MENEZES, J., MENEZES A. y VANSTONE, S.(2001). *The Elliptic Curve Digital Signature Algorithm (ECDSA).* Canadá: Universidad de Waterloo. p. 24-27. <http://cs.ucsb.edu/~koc/ccs130h/notes/ecdsa-cert.pdf>. [Consulta: 13 de abril de 2015]

[15] NEGRETE, M.A, GÓMEZ, K.P y RODRÍGUEZ-HERNÁNDEZ, F. (2006) *Inversión modular en Campos Finitos Binarios*, p. 2. <http://delta.cs.cinvestav.mx/~francisco/arith/Proyecto/Karla/ReporteLatex/ProyectoInversos.pdf> [Consulta: 5 de abril de 2015]

[16] NINTENDO. *Wii*. <https://www.nintendo.es/Wii/Wii-94559.html> [Consulta: 23 de mayo de 2015]

[17] PAE. *La Firma Electrónica*. Gobierno de España. <http://firmaelectronica.gob.es/Home/Ciudadanos/Firma-Electronica.html> [Consulta: 16 de junio de 2015]

[18] PÉRISSÉ, M.C. (2008). *Firma digital en la Web Semántica: Aplicación en la Biblioteca Digital*. Argentina. <http://www.cyta.com.ar/biblioteca/bddoc/bdlibros/cifrado_xml/cifrado_xml.htm> [Consulta: 16 de junio de 2015]

[19] INFORMATION SECURITY STACK EXCHANGE. *Rho*. <http://goo.gl/TDhB2a> [Consulta: 19 de junio de 2015]

[20] *Portal de la Facultad de Ingeniería Eléctrica de la Universidad Técnica Eslovaca en Bratislava. Proyecto ECDLP*. <http://ecdlp.aspone.cz/index.html> [Consulta: 19 de junio de 2015]

[21] *Portal oficial de la NSA*. <https://www.nsa.gov/ia/programs/suiteb_cryptography/>. [Consulta: 4 de abril de 2015]

[22] PREUKSCHAT, A. (2014) *Bitcoins y la criptografía de curva elíptica*. <http://www.oroyfinanzas.com/2014/01/criptografia-curva-eliptica-bitcoin-por-que-utiliza-ecdsa/> [Consulta: 4 de abril de 2015]

[23] PRZYBYLINSKI , P. (2014). "Experiencing the Quality of the Internet of Things.[en] Quality Digest. <http://www.qualitydigest.com/inside/quality-insider-article/experiencing-quality-internet-things.html> [Consulta: 22 de junio de 2015]

[24] DEL RÍO MATEOS, A. *Apuntes de criptografía*. Murcia: Universidad de Murcia, Facultad de matemáticas.

[25] SANTAMARÍA FERNÁNDEZ, J. (2012). *El logaritmo discreto y sus aplicaciones en criptografía*. Otras responsabilidades: Sadornil Renedo, D. Proyecto Final de Carrera. Cantabria: Universidad de Cantabria. p. 13-20,23-40. <http://repositorio.unican.es/xmlui/bitstream/handle/10902/3101/Jennifer%20Santamaria%20Fernandez.pdf?sequence=1> [Consulta: 26 de abril de 2015]

[26] SAORÍN, M. (2013). *Ecuaciones algebraicas*. Murcia: Universidad de Murcia, Facultad de matemáticas.

[27] SONY. *Play Station 3*. <https://www.playstation.com/es-es/explore/ps3/> [Consulta: 23 de mayo de 2015]

[28] TOVAR, S.A., VELÁZQUEZ, J. y GALLEGOS-GARCÍA, G. (2012). "Simulación del Estándar de Cifrado Avanzado para VoIP" en SG Buzz, Vol 37, agosto-octubre. <http://sg.com.mx/revista/simulaci%C3%B3n-del-est%C3%A1ndar-cifrado-avanzado-para-voip#.VSWbefmsVps> [Consulta: 11 de abril de 2015]

[29] TSCHOFENIG, H. y PÉGOURIE-GONNARD, M. (2015). "Performance Investigations" en IETF 92 (22-27 Marzo en Dallas, Texas). Disponible en <https://www.ietf.org/proceedings/92/slides/slides-92-lwig-3.pdf> [Consulta: 9 de marzo de 2015]

[30] DEL VALLE, A. (2010). *Geometría afín y euclídea*. Murcia: Universidad de Murcia, Facultad de matemáticas.

[31] WASHINGTON, L. C. (2008). *Elliptic Curves*, p. 1-34,143-154.

[32] WIKIADWYS. *Criptografía.* <http://wiki.adwys.es/index.php?title=Criptograf%C3%ADa> [Consulta: 16 de junio de 2015]

[33] WIKIPEDIA. *DMR.* <http://es.wikipedia.org/wiki/Gesti%C3%B3n_digital_de_derechos> [Consulta: 3 de abril de 2015]

[34] WIKIPEDIA. *DSA.* <http://es.wikipedia.org/wiki/DSA> [Consulta: 5 de abril de 2015]

[35] WIKIPEDIA. *RSA.* <http://es.wikipedia.org/wiki/RSA> [Consulta: 4 de abril de 2015]

[36] WIKIPEDIA. *SHA-1.* <http://en.wikipedia.org/wiki/SHA-1> [Consulta: 26 de mayo de 2015]