UNIVERSIDAD NACIONAL AUTÓNOMA
DE MÉXICO

FACULTAD DE CIENCIAS

CRIPTOGRAFÍA Y CURVAS ELÍPTICAS

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

M A T E M Á T I C O

P R E S E N T A :

CHRISTOPHER ROMÁN SILVA SARABIA

FACULTAD DE CIENCIAS
UNAM

DIRECTORA DE TESIS:
DRA. VERÓNICA MARTÍNEZ DE LA VEGA Y MANSILLA

2006

VNIVERSIDAD NACIONAL
AVTENOMA DE
MEXICO

ACT. MAURICIO AGUILAR GONZÁLEZ
Jefe de la División de Estudios Profesionales de la
Facultad de Ciencias
Presente

Comunicamos a usted que hemos revisado el trabajo escrito:

"Criptografía y curvas elípticas"

realizado por Christopher Román Silva Sarabia

con número de cuenta 09653484-5 , quien cubrió los créditos de la carrera de:
Matemáticas

Dicho trabajo cuenta con nuestro voto aprobatorio.

Atentamente

Director de Tesis Propietario	Dra. Verónica Martínez de la Vega y Mansilla
Propietario	Dr. Alejandro Illanes Mejía
Propietario	Dr. Javier Páez Cárdenas
Suplente	Mat. Julio César Guevara Bravo
Suplente	M. en C. María de la Asunción Preisser Rodríguez

Consejo Departamental de Matemáticas

M. en C. Alejandro Bravo Mojica

FACULTAD DE CIENCIAS
CONSEJO DEPARTAMENTAL
DE
MATEMATICAS

Dedicatoria

A mis padres y mis hermanos.

A mis tíos, tías, primos, primas, sobrinos y sobrinas

A mis niñas (Alyna, Moni y Meredith).

A mis amigos.

A las maestras Asunción, Diana, Socorro y Vero.

A los que ya no están. Mis abuelos (Rip), Corona (Rip), mi tía Maui (Rip), al profesor Vivar (Rip), al maestro Saleano (Rip).

Agradecimientos

Ha sido mucho el tiempo que le he dedicado a terminar está carrera, pero afordunadamente ha sido mas el tiempo que me han dedicado muchas personas hasta este día, los cuáles son parte de este logro también, por lo que quiero agredecerles a continuación.

Al Ingeniero y la Señora (mis padres) guías y ejemplo a lo largo de estos años, darles gracias por la dedicación y paciencia que han tenido conmigo y con mis hermanos a lo largo de estos años.

A mis hermanos agradecerles su apoyo en los momentos que lo he necesitado.

A la familia Sarabia Sanchez, agradecerles por abrirme las puertas de su casa cuando lo he necesitado y por él apoyo brindado a mis padres, a mí y mis hermanos, en especial a Doña Francisca, Doña Mona y a mi tío Pedro por su ayuda en los momentos díficiles y estar al tanto de mí.

También agradecerles a Adrián y al tío Pancho por su ayuda los cuales considero parte de mi familia. Así como a mis hermanos Eduardo y Román, gracias por aguantarme y por estos años de amistad.

A mis brothers Alex, Erubiel, Germán, Jorge, Lorenzo, Rogelio y Sergio y a las sisthers Claudia, Lupita, Mayra y Vero gracias por su amistad, en particular a Germán y Jorge que son los que me hablan para ir a las reuniones y se han encargado de que siempre regrese bien a mi casa.

A mis muy buenos amigos Javier, Eduardo y Alfredo por ayudarme con mis estudios durante distintas etapas.

A toda la banda de biologos (Armando, Carmen, Clemen, Demián, Isabel, Ivonne, Javier, Leti, Miguel, etc.) por brindarme su amistad y aceptarme como uno mas de ustedes.

Agradecerles a mis maestros su dedicación por tratar de que aprendiera un poco de lo que ellos saben como a la maestra socorro en mi educaión básica. A los maestros Alejandro Illanes y Javier Paez por su valiosa colaboración para corregir todos los errores en está tesis. A la maestra Diana Maya por por sus enseñanzas en distintas materias en especial en geometría, la cuál me ayudo a comprender. A la maestra Asunción Preisser por su amistad, por transmitirme un poco de su conocimiento de la Lógica y por permitirme trabajar con ella estoso últimos años.

Finalmente agradecerle a la Dra. Verónica Martínez por la infinita paciencia, dedicación, tiempo y colaboración para la realización de este trabajo, el cuál no habría podido terminar sin su ayuda.

Índice General

Capítulo 0

INTRODUCCIÓN

La criptografía, como se definirá en el capítulo 1, es el arte y ciencia de escribir en forma oculta informaciones confidenciales, de tal manera que éstas sólo puedan ser leídas por las personas deseadas.

Como una muestra coloquial de ello tenemos la sección de empleos en los periódicos. Algunas empresas han decidido escribir sus oportunidades de trabajo en un lenguaje distinto al español, de tal manera que la empresa logra el objetivo de que su mensaje llegue a cierto tipo de personas, aquellas que conocen ese lenguaje. Con esto aseguran que las personas que solicitarán la vacante cumplan con este requisito.

Otro ejemplo es la escritura (o simbología) plasmada en los distintos tipos de pirámides antiguas, la mayoría de nosotros desconocemos los mensajes escritos ahí, más aún, la mayoría de los especialistas en estas culturas sólo tienen interpretaciones de estos mensajes pero no están cien por ciento seguros de que sus interpretaciones sean correctas.

En fin, como éstos podríamos dar varios ejemplos. En el capítulo 1, dentro de la reseña histórica, daremos ejemplos menos coloquiales y en los que las matemáticas juegan un papel importante.

Inicialmente me interesé en conocer algunos métodos para ocultar mensajes, pero conforme investigué sobre el tema pude darme cuenta de que la evolución de la criptografía ha llegado a niveles muy avanzados. En un principio se usaron algunos métodos sencillos en los que se hacían cambios de una letra por otra. Estos tipos de métodos se pueden ver como problemas de teoría de grupos y teoría de números. Posteriormente, se utilizaron estos mismos tipos de cambios, pero ahora utilizando bloques de letras (por ejemplo se separa el texto en pares de letras y a cada primer letra de cada bloque se le aplica un método de cambio y a las segundas letras otro tipo de cambio de letras distinto del primero).

Después se empezaron a hacer máquinas exclusivamente para este fin, las cuales tuvieron su mayor auge en la segunda guerra mundial. Más recientemente se empezaron a utilizar métodos que hacen uso de problemas de díficil solución o problemas para los cuales se requiere de mucho tiempo para resolverlos. De algunos de estos problemas se hace una revisión en el capítulo 2.

Hasta este punto los metódos utilizados se pueden ver como problemas para los cuales se utilizan la teoría de grupos y la teoría de números tanto para su descripción como para su solución. En las últimas décadas se han hecho propuestas de nuevos métodos de encriptación. Dentro de las propuestas que se han hecho, están las que utilizan para este fin las redes neuronales, la utilización de fotones (criptografía cuántica) y la manera que describiré en esta tesis, que es por medio de curvas elípticas.

En sí los métodos basados en curvas elípticas tienen como predecesores a algunos modelos basados en la teoría de números y en la teoría de grupos. Esto se debe a que las curvas elípticas tienen una estructura de grupo, por lo que se logran hacer ciertas analogías entre las curvas elípticas y los grupos utilizados en los modelos basados en la teoría de números. Por esta razón se pueden ver algunos de estos modelos utilizando curvas elípticas.

Por lo anterior, en el capítulo 3, se hará una exposición completa pero a la vez sencilla de las curvas elípticas. Hago mención de que es completa ya que se analizarán en principio las propiedades de las curvas elípticas en el campo real, para después hacer un análisis de las curvas elípticas en distintos campos. Pero a la vez trato de hacer un manejo sencillo, ya que las curvas elípticas, en general, se ven como un objeto en el espacio proyectivo, lo cual

en el momento de hacer mi investigación se me hizo demasiado complicado. Por ello opté por ver mejor a las curvas elípticas como un objeto en $\mathbb{R}^2 \bigcup \{\infty\}$ donde es más fácil trabajar y a partir de esto dar el paso a otros campos.

Por lo anterior esta tesis quedo estructurada de la siguiente manera.

Capítulo 1.
Se presentan algunos datos históricos sobre la criptografía además de la definición de lo que es la criptografía y definiciones relacionadas con este tema

Capítulo 2.
En este capítulo se ilustran algunos de los métodos criptográficos mas conocidos desde los de sustitución como el método de Cesar, el de alfabeto diezmado, la encriptación afin, así como algunos métodos mas complicados como el método de matrices y algunos de llave pública dentro de los que estan el RSA, el Massey-Omura y El Gamal, en donde, para cada método, se revisa un ejemplo en concreto.

Capítulo 3.
Aquí se muestra la definición de curvas elípticas y posteriormente se hace un desarrollo de éstas en distintos campos, desde mi punto de vista se hace un muy buen análisis de las curvas elípticas en el campo complejo.

Capítulo 4.
Finalmente en este capítulo se desarrolla la encriptación en curvas elípticas, se muestran ejemplos de algunas construcciones que se necesitan para poder hacer la encriptación como, por ejemplo, calcular la suma de un punto k veces en la curva; pasar el texto a puntos en la curva y ejemplos concretos de encriptación en la curva elíptica por medio de dos métodos.

Apéndice A.
Aquí se presentan algunas definiciones que serán básicas sobre la teoría de los números y que se utilizarán a lo largo de la tesis.

En principio esta tesis estaría dirigida a alumnos de matemáticas o de ciencias de la computación con conocimientos básicos de teoría de números y un poco de teoría de grupos y de anillos, salvo la sección 3.3 para la cual se necesita una base sólida tanto de variable compleja como de teoría de grupos

y de anillos. Debo de agregar que en este trabajo no busco decidir cual de los métodos que se describirán es mas eficaz, así como tampoco analizar cual de estos métodos es más rápido, si no únicamente se pretende hacer la descripción de algunos métodos de encriptación, en particular los que hacen uso de curvas elípticas.

Capítulo 1

CRIPTOGRAFÍA: DEFINICIÓN E HISTORIA

Uno de los matemáticos que más aportaciones hizo a la teoría de los números es el inglés Godfrey H. Hardy, el cual se ufanaba de que sus descubrimientos y, en general, la teoría de números no tenía ninguna aplicación. Esto lo manifestaba cada vez que tenía oportunidad. Por ejemplo, en el Teorema 2.10 de su libro *A Mathematical Apology*, después de probar el viejo teorema que establece que el número de primos es infinito menciona que éste sólo tiene una ligera importancia práctica. A pesar de sus opiniones, con el paso de los años los matemáticos fueron descubriendo algunas aplicaciones interesantes de esta teoría.

En la actualidad, se ha descubierto que el conocimiento de los primos es fundamental en la teoría de la criptología (el estudio de los sistemas secretos de escritura).

La criptología se divide en dos ramas antagonistas, la *criptografía* y el *criptoanálisis*. La palabra criptografía se deriva de las palabras griegas *kriptos*, que quiere decir oculto, y *graphein*, que significa escribir. La criptografía

entonces es el arte y ciencia de escribir en forma oculta las informaciones confidenciales (excepto para las personas deseadas). Por el contrario, el criptoanálisis es el encargado de romper las claves que se usan en los mensajes secretos, para que las personas que no son las destinatarias de los mensajes sean capaces de conocer su contenido. En este trabajo desarrollaremos algunas técnicas matemáticas que se usan para la criptografía.

Con esta idea, siempre estaremos pensando en que tenemos un mensaje que queremos enviar, a estos mensajes les llamaremos *textos planos*, veremos cómo se disfraza éste para transformarlo en un *texto cifrado* o *texto encriptado*. Estos últimos son escritos usando algún alfabeto consistente de un cierto número de N letras, lo de letras es sólo una manera de llamarlas pues se pueden usar toda clase de símbolos como las letras que usamos regularmente, también pueden ser números, espacios en blanco, símbolos de puntuación, números o cualquier otro símbolo que queramos usar.

El proceso de convertir un texto plano en un texto cifrado es llamado *ciframiento* o *encriptación* (usaremos estos nombres indistintamente) y al proceso inverso se le conoce por *desciframiento* o *desencriptación* (también usaremos estas palabras sin distinción). Un *cifrado* o *ciframiento* es un método para cambiar un texto plano en un texto cifrado. Una *llave* o *clave* es el elemento que permite saber cómo fue encriptado un mensaje, así la tarea del criptoanalista consiste en descubrir la llave, y con esto allanar el camino para encontrar el texto plano.

Una *función de encriptación* es una función que toma cualquier texto plano y lo transforma en un mensaje cifrado. Nosotros supondremos que nuestra función (f) es una función uno a uno. La transformación de desencriptación es entonces la función inversa (f^{-1}), que recupera el texto plano a partir del texto cifrado.

El siguiente diagrama ilustra esta situación:

$$\mathbf{P} \xrightarrow{f} \mathbf{E} \xrightarrow{f^{-1}} \mathbf{P}$$

A cualquier f de este tipo le llamaremos un *sistema criptográfico*.

A lo largo de la historia, desde hace muchos siglos, la criptografía ha servido para encubrir información, ya que por diversas razones los seres humanos han estado interesados en proteger cierta información. Por ejemplo los asirios estaban interesados en mantener en secreto la fabricación de

la céramica, los chinos se interesaron en guardar en secreto el método de la fabricación de la seda, los alemanes durante la segunda guerra mundial trataron de proteger sus secretos militares con su famosa máquina Enigma. En épocas más recientes, las instituciones e industrias gubernamentales de Estados Unidos se han apoyado en la criptografía para mantener en secreto determinada información, pero debido al adelanto de las computadoras y la interconectividad, son sujetos frecuentemente a ciberataques, además de sufrir intrusiones en sus sistemas y espionaje industrial.

A continuación daremos una breve cronología de la historia de la criptografía.

Cerca de 1900 a.C., un escribano egipcio utilizó jeroglíficos no estándares en una inscripción. Kahn enumera esto como el primer ejemplo documentado de la criptografía escrita.

En 1500 a.C., antiguos comerciantes asirios utilizaron lo que se le llamo la *La talla*, lo cual es un pedazo de piedra plana dentro del cual, tallaron una mezcla de imágenes, además de utilizar cierta escritura con lo cual identificaban las transacciones que hacían. Derivado de este mecanismo, produjeron lo que conocemos en nuestros días como la "Firma". La gente en general sabía que una firma en particular pertenecía a un determinado comerciante, debido a que solamente él tenía la forma de producirla.

Entre los años 500 y 600 a.C., los escribanos hebreos que escribian el libro de Jeremiah utilizaron en lugar del alfabeto normal un alfabeto al revés, lo cual es una forma simple de sustitución, este alfabeto fue conocido como ATBASH.

El emperador Julio Cesar (100-44 a.C.) utilizó una substitución simple con el alfabeto normal, lo utilizaba para comunicaciones de gobierno, debido a que no confiaba en sus mensajeros. Este cifrado era menos fuerte que ATBASH, por muy poco, pero en un tiempo en que pocas personas leían era bastante bueno. El método consistía en sustituir cada letra del alfabeto por la que se encontraba tres lugares a la derecha, en nuestro alfabeto sería substituir cada A en el texto por una D, cada B por una E, y así sucesivamente. También utilizó la transcripción del latín al griego, además de otros cifrados simples.

En 1379, Gabrieli di Lavinde, a petición de Clemente VII, compila un alfabeto que nace de la combinación del Alfabeto de sustitución y un código

pequeño. Esta clase de código-cifrado fue usado en general entre diplomáticos y algunos civiles por los próximos 450 años, a pesar del hecho de que ya había métodos de cifrado más fuertes inventados en aquel tiempo.

En 1466, Leon Battista Alberti (un amigo de Leonardo Dato, un secretario pontificio que pudo haber instruido a Alberti en las técnicas más avanzadas de la criptología) inventó y publicó el primer cifrador polialfabético, éste constaba de un disco de cifrado (conocido por nosotros como el Captan Midnight Decoder Badge) para simplificar el proceso. Esta clase de cifrado fue usado aparentemente hasta el año 1800. Alberti también escribió extensamente sobre los distintos métodos de cifrado conocidos hasta aquel entonces, además de escribir sobre el de su propia invención. Alberti también utilizó su disco para cifrar códigos. El sistema creado por Alberti era mucho más fuerte que la nomenclatura que usaban los diplomáticos en ese entonces y que siguieron usando durante siglos.

En 1518, Johannes Trithemius escribió el primer libro impreso usando criptología. En él hace usó de distintos tipos métodos de encriptación, como por ejemplo un cifrado esteganográfico (es decir, de ocultar la escritura) en el cual cada letra fue representada como una palabra tomada de una sucesión de columnas o por ejemplo en el que a cada letra le asignaba otra letra.

En 1553, Giovan Batista Belaso introdujo la noción de usar una frase como la clave para una encifrado polialfabético repetido. Éste es el encifrado polialfabético estándar llamado *"Vigénere"* por la mayoría de los escritores hoy en día.

En 1563, Giovanni Battista Porta escribió un texto cifrado, introduciendo el cifrado digráfico. Clasificó cifras en transposición, la substitución y substitución de símbolos (usados de un alfabeto extraño). También sugirió el uso de sinónimos y de faltas de ortografía para confundir al criptoanalista y al parecer introdujo la noción de un alfabeto mezclado en una tabla polialfabética.

En 1585, Blaise de Vigenére escribió un libro en cifras, incluyendo los primeros sistemas auténticos de documentos y de cifrado de textos para documentos usados como claves actuales de documentos.

En 1623, Sir Francis Bacon describió un cifrado que hoy lleva su nombre - un cifrado biliteral, conocido hoy como codificación binaria 5-bit -.

En 1790, Thomas Jefferson, ayudado posiblemente por el Dr. Robert Patterson (matemático de la Universidad de Pennsilvania.), inventó su cifrado de la rueda. Ésta fue reinventada en varias formas más adelante y utilizada en la segunda guerra mundial por la marina de los E.E.U.U. (conocido como el cifrado de la tira, M-138-A).

En 1917, William Frederick Friedman, quien fue honrado más adelante con el nombre de el padre del criptoanálisis de los E.E.U.U. (y el hombre que acuño ese término), fue empleado como criptoanalista civil (junto con su esposa Elizabeth) en los laboratorios de Riverbank, además realizó criptoanálisis para el gobierno de los E.E.U.U., que no contaba propiamente con ningún experto criptoanalista. Friedman comenzó una escuela para los criptoanálistas militares en Riverbank. Más adelante se transladó a Washington.

Entre los años de 1933-1945 la máquina Enigma no era un éxito comercial pero Alemania asumió el control y la mejoró hasta convertirla en el caballo de batalla criptográfico de la Alemania nazi. Pero la manera de descifrar los mensajes fue descubierta por el matemático polaco, Marian Rejewski, basado solamente en un texto cifrado que capturaron y una lista de las claves diarias de tres meses obtenidas a través de un espía.

En el año de 1976 un diseño creado por IBM, basado en el cifrado de Lucifer y con cambios hechos por la N.A.S.A. de los E.E.U.U. (los cuales incluyeron mejoras a la caja S y la reducción del tamaño dominante), fue elegido para ser el cifrado de datos estándar de los Estados Unidos. Este método ha tenido la aceptación mundial, en gran parte porque se ha demostrado fuerte contra 20 años de ataques.

En 1976 Whitfield Diffie y Martin Hellman publicaron "New directions in cryptography", introduciendo la idea de la clave pública de la criptografía. También pusieron adelante la idea de la autentificación por potencias de una función unidireccional. Cerraron el documento con la siguiente observación "la habilidad en la producción del criptoanálisis ha estado siempre en el lado de los profesionales, pero la innovación, particularmente en el diseño de los nuevos tipos de sistemas criptográficos, ha venido sobre todo de amateurs."

En 1977 inspirados por los documentos de Diffie-Hellman y siendo principiantes en la criptografía, Ronald L. Rivest, Adi Shamir y Leonard M.

Adleman discutieron cómo hacer un práctico y público sistema de cifrado. Una noche en abril, Ron Rivest se levantó con un dolor de cabeza masivo y el algoritmo de RSA vino a él. Él lo escribió y lo envió a Shamir y Adleman; a la mañana siguiente. Era un práctico cifrado público para ambos, enviado confidencialmente con todo y las firmas digitales, basado en la dificultad de descomponer números muy grandes en sus factores primos. Sometieron esto a Martin Gardner el 4 de abril para la publicacin en Scientific American. El artículo apareció en Scientific American en el año de 1977 en su edición de septiembre, en este se incluyó una oferta para enviar el informe técnico completo a cualquier persona que lo solicitase. Hubo millares de peticiones de todo el mundo.

En 1990, Xuejia Lai y James Massey en Suiza publicaron "A Proposal for a New Block Encription Standard", un algoritmo internacional propuesto del cifrado de datos (IDEA) que pudiera sustituir el DES. La IDEA usa una clave de 128 bits y emplea operaciones que son convenientes para las computadoras con fines generales, por lo tanto hizo prácticamente más eficiente el software.

En 1991 Phil Zimmermann lanzó su primera versión de PGP (Pretty Good Privacity) en respuesta a la amenaza del FBI de exigir el acceso a las comunicaciones de los ciudadanos. La PGP ofreció alta seguridad en las comunicaciones de los ciudadanos en general y como tal se habría podido considerar como un competidor a los productos comerciales como Mailsafe de RSADSI.

Sin embargo, el PGP es especialmente notable porque fue lanzado como freeware y se ha convertido en un estándar mundial mientras que sus competidores de la época siguen siendo altamente desconocidos.

En 1994, el profesor Ron Rivest, autor de los algoritmos anteriores RC2 y RC4 incluidos en la biblioteca criptográfica de RSADSI's BSAFE, publicó un algoritmo propuesto, RC5, en el Internet.

Este algoritmo utiliza la rotación dato-dependiente como su operación no lineal y da parámetros de modo que el usuario pueda variar el tamaño de bloque, el número de redondeo y la longitud dominante. Sigue siendo demasiado nuevo para ser analizado completamente y para permitir saber

qué parámetros utilizar para una fuerza deseada. Aunque un análisis realizado por los laboratorios de RSA, divulgados en CRYPTO'95, sugiere ciertos valores con los que se logra un mejor desempeño. Debe recordarse, sin embargo, que esto es sólo un primer análisis.

En las siguientes secciones veremos algunos sistemas criptográficos, empezaremos por algunos de sustitución *monoalfabética*, los cuales consisten en cambiar letra por letra en un texto plano. Después veremos los sistemas de *encriptación por bloques*, los cuales trabajan sustituyendo las letras por pares, tercias, o en general por bloques de n letras. Finalmente veremos el sistema de encriptación más usado en la actualidad, el sistema RSA, el cual se desarrollará en forma de encriptación momoalfabética aunque también puede hacerse en bloques.

Capítulo 2

CRIPTOGRAFÍA

2.1. ENCRIPTACIÓN POR SUSTITUCIÓN MONOALFABÉTICA

En un sistema de encriptación monoalfabético lo que se hace es sustituir cada letra usada en el texto plano por otra letra de manera que la transformación sea inyectiva (uno a uno), es decir, a cada letra le corresponde una y solo una letra. De esta manera, tendremos una asignación biunívoca entre las letras usadas del texto plano y las letras usadas en el texto cifrado.

Podemos entonces observar que si tomamos una letra de las usadas en el texto plano, y sólo usamos letras en español para encriptar, tenemos 27 posibilidades de asignarle una letra del alfabeto. Al tomar una segunda letra de las usadas en el texto plano, ya sólo tendremos 26 posibilidades para asignarle una letra del alfabeto (ya que no podemos volver a usar la primera). Para la tercera letra tenemos 25 opciones, para la cuarta 24, etc. Con lo anterior podemos notar que tenemos 27! posibles sistemas de encriptación distintos de sustitución monoalfabética.

A continuación describiremos, en forma más detallada, la manera en que se hace el proceso de encriptación y desencriptación por sustitución monoalfabética, para después ver algunos de los casos particulares de los 27! posibles.

Lo primero que se hace es asignarle un número a cada letra del alfabeto. Para los sistemas criptográficos que veremos en esta sección numeraremos las letras de la A a la Z por su respectivo número ordinal entre 0 y 26, como se muestra a continuación.

Texto Plano	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Ordinal	0	1	2	3	4	5	6	7	8	9	10	11	12	13

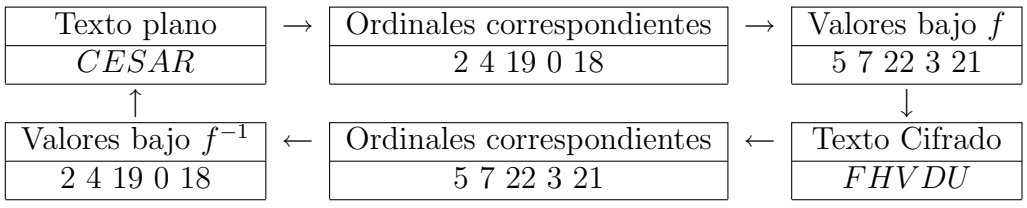
Texto Plano	$\tilde{N}$	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ordinal	14	15	16	17	18	19	20	21	22	23	24	25	26

Usando este esquema, lo que se hace en una sustitución monoalfabética es lo siguiente. Se da una biyección f del conjunto $\{0, 1, 2, ..., 26\}$ en sí mismo.

Ahora, dado un texto plano, se cambia cada una de sus letras por su ordinal correspondiente, a continuación, cada uno de los ordinales n se cambia por el ordinal $f(n)$, y finalmente se cambia el ordinal $f(n)$ por la letra que le corresponde. De esta manera se obtiene el texto encriptado.

Si uno quiere desencriptar el mensaje, se hacen las operaciones inversas, es decir: a cada letra del texto encriptado, se le asigna su número ordinal m, entonces se obtiene el número ordinal $f^{-1}(m)$, y se pone la letra que le corresponde. De esta manera recuperaremos el mensaje original.

En la siguiente gráfica se ilustra el proceso descrito en los dos párrafos anteriores, donde se usa la función f que a cada ordinal n le suma 3 módulo 27.



2.2. MÉTODO CÉSAR

Este método de encriptación recibe el nombre de César porque el mismo emperador Julio César lo usaba para comunicarse con sus generales. La manera como trabaja es simplemente la sustitución de una letra por la letra que se ubica tres lugares después en el alfabeto (módulo 27). La siguiente tabla dice cómo se cambian las letras.

Texto Plano	A	B	C	D	E	F	G	H	I
Texto Cifrado	D	E	F	G	H	I	J	K	L

Texto Plano	J	K	L	M	N	$\tilde{N}$	O	P	Q
Texto Cifrado	M	N	$\tilde{N}$	O	P	Q	R	S	T

Texto Plano	R	S	T	U	V	W	X	Y	Z
Texto Cifrado	U	V	W	X	Y	Z	A	B	C

Arriba ya mostramos cómo se cambia la palabra $CESAR$ con este método. Aquí ni siquiera tenemos que hacer tanto ruido con la función f. Simplemente, para cifrar un mensaje, tomamos cada letra por la letra que aparece en el reglón inferior de la tabla. De esta manera la palabra $CESAR$ se cambia por la palabra $FHVDU$. Y para recuperar el mensaje original simplemente cambiamos cada letra de la nueva palabra por su correspondiente en el renglón de arriba.

Si queremos usar el lenguaje de las funciones, para el método César usaríamos la función $f(n) = m$, donde m es el residuo que resulta de dividir $n + 3$ entre 27. Así que

$$f(n) \equiv n + 3 (\text{mod } 27).$$

Claramente la función f^{-1} queda dada por restar 3 módulo 27. Entonces $f^{-1}(m)$ es el residuo que se obtiene al dividir el número $m - 3$ entre 27. De modo que

$$f^{-1}(m) \equiv m - 3 (\text{mod } 27).$$

Así como César usaba una traslación de 3 lugares en las letras, se podría usar una traslación de k lugares, para cualquier $k \in \{1, 2, ..., 26\}$. Así por ejemplo, si usamos $k = 5$, la palabra $CESAR$ se cambia por la palabra $HJXFW$ y la función se puede representar en forma abreviada por las fórmulas:

$$\begin{aligned} f(n) &\equiv n + 5 (\text{mod } 27) \text{ y} \\ f^{-1}(m) &\equiv m - 5 (\text{mod } 27). \end{aligned}$$

O más generalmente,

$$\begin{aligned} f(n) &\equiv n + k (\text{mod } 27) \text{ y} \\ f^{-1}(m) &\equiv m - k (\text{mod } 27). \end{aligned}$$

A pesar de que en algún tiempo se usó el método César, ahora resulta demasiado simple para que sirva de algo. Simplemente hay sólo 26 posibilidades de obtener el cifrado. Bastaría con que uno las probara todas para encontrar el mensaje oculto. Por esta razón se han inventado métodos más complicados. Veamos otros ejemplos.

2.3. MÉTODO DEL ALFABETO DIEZMADO

Para tener más métodos, ahora podríamos multiplicar en lugar de sumar. Es decir, podríamos usar la regla (aquí k es un número fijo).

$$f(n) \equiv kn (\text{mod } 27).$$

Claro que ésta es sólo una forma simbólica de representar el método. Lo que en realidad tendríamos que decir es que dada n, $f(n)$ es el residuo que se obtiene de dividir a kn entre 27.

Para que este método sirva, como dijimos antes, la función f debe ser inyectiva. De modo que se debe tener la implicación

$$f(n) = f(m) \Rightarrow n = m.$$

O, equivalentemente,

$$kn \equiv km(\text{mod } 27) \Rightarrow n = m \text{ (para números } n, m \text{ en}\{0, 1, 2, ..., 26\}).$$

De nuestros conocimientos de divisibilidad sabemos que esta implicación se puede garantizar si (y sólo si) k es primo relativo con 27. Pues en este caso k tiene un inverso multiplicativo módulo 27.

Este método usa la palabra *diezmado* porque diezmar significa eliminar uno de cada diez y en este método, lo que se hace es tomar sólo uno de cada k símbolos, pues se usan los números, k, $2k$, $3k$, $4k, ...$

Para ejemplificar, a continuación ponemos la tabla que serviría para transformar los textos usando este método, cuando $k = 5$.

Texto Plano	A	B	C	D	E	F	G	H	I
Ordinal	0	1	2	3	4	5	6	7	8
Ordinal por 5	0	5	10	15	20	25	30	35	40
Ordinal mod 27	0	5	10	15	20	25	3	8	13
Texto Cifrado	A	F	K	O	T	Y	D	I	N

Texto Plano	J	K	L	M	N	$\tilde{N}$	O	P	Q
Ordinal	9	10	11	12	13	14	15	16	17
Ordinal por 5	45	50	55	60	65	70	75	80	85
Ordinal mod 27	18	23	1	6	11	16	21	26	4
Texto Cifrado	R	W	B	G	L	P	U	Z	E

Texto Plano	R	S	T	U	V	W	X	Y	Z
Ordinal	18	19	20	21	22	23	24	25	26
Ordinal por 5	90	95	100	105	110	115	120	125	130
Ordinal mod 27	9	14	19	24	2	7	12	17	22
Texto Cifrado	J	$\tilde{N}$	S	X	C	H	M	Q	V

También a modo de ejemplo, notemos que la palabra $AJEDREZ$ se transformaría en la palabra $ARTOJTV$.

Ya que $5 \cdot 11 = 55 \equiv 1(\text{mod } 27)$, el inverso de 5 módulo 27 es el número 11. Así que podemos representar a la función inversa f^{-1} por:

$$f^{-1}(m) \equiv 11 \cdot m(\text{mod } 27)$$

Por supuesto que no tenemos que estar multiplicando por 11 cuando ya tenemos la tabla, pues simplemente para decifrar un mensaje, tenemos que localizar cada una de las palabras del mensaje cifrado en el renglón de abajo de la tabla y sustituirla por la letra que se encuentra arriba de ella.

Dado que hay 18 números k en $\{0, 1, 2, ..., 26\}$ que son primos relativos con 27, tenemos ahora 17 métodos diferentes de encriptar (no se toma en cuenta $k = 1$, pues con esto los mensajes no se cambian nada).

2.4. MÉTODO DE ENCRIPTACIÓN AFÍN

Este método es una simple combinación de los dos anteriores. La fórmula que representa este método está dada por

$$f(n) \equiv a \cdot n + k(\text{mod } 27)$$

Como siempre, a y k son números fijos. Y como vimos en el método anterior, aquí se necesita pedir que a sea un número primo relativo con 27, pues con esto se puede garantizar que la función f es biyectiva, esto se da porque, en estos casos, a tiene un inverso módulo 27. Entonces la función inversa puede representarse con la fórmula

$$f^{-1}(m) \equiv a^{-1}(m - k)(\text{mod } 27)$$

Combinando estos dos métodos obtenemos un total de $18 \cdot 27 - 1$ métodos de encriptado. Ponemos el -1 porque se pueden tomar en cuenta todas las combinaciones posibles para a y k excepto la combinación $a = 1$ y $k = 0$ pues ésta no cambia las letras y entonces no representa ninguna manera de encriptar mensajes.

A pesar de contar ahora con 485 métodos, estos métodos siguen siendo muy simples, son muy fáciles de decifrar. De hecho, no importa que función inyectiva $f : \{0, 1, 2, ..., 26\} \to \{0, 1, 2, ..., 26\}$ se tome, el método de

sustitución monoalfabética que usa a f es relativamente fácil de ser decifrado cuando se usa para un texto largo o para varios textos. Esto se hace como sigue.

Observe usted un texto largo cifrado usando alguna f. En él cada letra del texto original (o plano) se ha cambiado por otra letra del alfabeto. Cuente cuántas veces aparece cada letra. Se sabe la probabilidad de que cada letra aparezca en un texto normal en español y hasta hay tablas describiendo esto. Por ejemplo, la siguiente es una tabla compilada por H. Beker y F. Piper, en ella aparece el porcentaje de veces en que aparecen las respectivas letras en los textos en inglés que ellos analizaron (revisaron textos que en total sumaron más de 100,000 letras).

Letra	A	B	C	D	E	F	G	H	I
Porcentaje	8,2	1,5	2,8	4,3	12,7	2,2	2,0	6,1	7,0

Letra	J	K	L	M	N	$\tilde{N}$	O	P	Q
Porcentaje	0,2	0,8	4,0	2,4	6,7	??	7,5	1,9	0,1

Letra	R	S	T	U	V	W	X	Y	Z
Porcentaje	6,0	6,3	9,1	2,8	1,0	2,4	0,2	2,0	0,1

De acuerdo con esto, la letra que más se usa es la E, seguida de la T, la A y la O. De modo que si en el texto cifrado que tenemos sustituimos la letra que más aparezca por la E, la segunda que más aparezca por la T y la tercera por la A, tendremos una alta probabilidad de acertar. Pero si no se puede empezar en otro orden combinando estas letras y sustituyéndolas con las que más aparecen en el texto cifrado. De esta manera, tendremos posibilidades de empezar a jugar como en el juego del ahorcado. Podemos hacer uso de otros hechos, como el de que la E muchas veces va acompañado de la L, la N o la S. Jugando con estas posibilidades, podremos acertar y descubrir nuevas palabras en el texto y cuáles son las letras que les corresponden a ciertas letras. Podemos continuar usando la O y la I, exactamente como en el ahorcado y usando asociaciones de ideas como en el juego del ahorcado terminar por decifrar el mensaje. La ayuda de una computadora que permite cambiar todas las letras de un tipo por letras de otro tipo sería de gran ayuda y permitiría decifrar el texto muy rápidamente. Por la facilidad con

que se pueden decifrar los mensajes cifrados usando la encriptación monoalfabética es que se han inventado una gran cantidad de otros métodos. En este trabajo describiremos algunos de los que más se usan actualmente.

2.5. MÉTODO DE MATRICES

Para este método, necesitamos trabajar con un número primo como módulo. Así que en lugar de 27 podríamos usar el 37. Esto nos permitiría incluir las 27 letras y los 10 dígitos.

Una vez que hemos separado nuestro texto plano en bloques de n letras podemos asignarle a cada letra su número ordinal correspondiente con lo que tendríamos ahora bloques de n números, a cada bloque de n números lo podemos ver como un vector de n entradas de la forma

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$$

Para obtener un texto cifrado, podríamos hacer n combinaciones lineales de los números a_i. (todo esto módulo 37, por supuesto), de tal modo que obtengamos valores b_j. De esta manera obtenemos la siguiente serie de congruencias:

$$\begin{gathered} c_{11}a_1 + c_{12}a_2 + \cdots + c_{1n}a_n \equiv b_1 (\text{mod } 37) \\ c_{21}a_1 + c_{22}a_2 + \cdots + c_{2n}a_n \equiv b_2 (\text{mod } 37) \\ \vdots \\ c_{n1}a_1 + c_{n2}a_2 + \cdots + c_{nn}a_n \equiv b_n (\text{mod } 37) \end{gathered}$$

Por supuesto que esto lo podemos poner, con notación matricial, de la siguiente forma:

$$\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \equiv \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

Para que esto funcione, tenemos que proponer una matriz invertible. De esta manera tendremos una correspondencia biyectiva y podremos reconstruir un mensaje simplemente multiplicando por la matriz inversa. Para esto pedimos que el módulo sea un número primo. Pues de esta manera, al trabajar con los números $\{0, 1, 2, ..., 36\}$, y la suma y el producto módulo 37, tendremos un campo y entonces toda la teoría de matrices funciona adecuadamente. En particular, para comprobar que la matriz de las $c_{i,j}$ sea invertible, simplemente tendremos que comprobar que su determinante sea distinto de 0 modulo 37.

Ahora veremos otra forma de encriptar textos en bloques usando el mejor método que se conoce.

2.6. MÉTODO RSA

Uno de los más viejos problemas de la teoría de los números es el de encontrar un algoritmo eficiente para factorizar números (naturales). En principio parecería que este problema no es tan difícil de resolver pues desde la escuela primaria nos enseñan cómo hacerlo. Recordemos cómo se hace. Tomamos un número natural n y tomemos el primer número primo (el 2). Si 2 divide a n, tomamos ahora el número $\frac{n}{2}$ y revisamos si 2 divide a $\frac{n}{2}$. En el caso en que esto ocurra, consideramos ahora el número $\frac{n}{2^2}$ y seguimos con este proceso hasta encontrar una potencia 2^k del número 2 tal que $\frac{n}{2^k}$ ya no sea divisible entre 2. Ahora tratamos con el siguiente primo (el 3) y hacemos el proceso hasta encontrar una potencia 3^m del número 3 tal que el número $\frac{n}{2^k 3^m}$ ya no sea divisible entre 3. Notemos que puede ocurrir que $k = 0$ y/o que $m = 0$ que corresponde a los casos en que el 2 (y/o el 3) mismo no divida a n (y/o a $\frac{n}{2^k}$). Continuamos este proceso con todos los primos menores o iguales que n, y al final, la factorización de n será $n = 2^k 3^m ...$

Este proceso tan simple que hemos hecho muchas veces tiene sus bemoles cuando el número n es muy grande. Aun para las computadoras actuales, factorizar con este método, un número inicial n que conste de 200 cifras o más y que tenga pocos factores primos, es casi imposible hacerlo en un tiempo razonable. Esta dificultad y el Pequeño Teorema de Fermat son la base para el sistema de encriptado RSA. Expliquémonos.

El sistema RSA fue inventado por Rivest, Shamir y Adleman en 1977. La principal idea atrás de este sistema es que es relativamente fácil hallar números p y q de 100 cifras que tienen una alta probabilidad de ser primos y que sin embargo es muy difícil factorizar el producto pq que contará con casi 200 cifras. Los valores de 100 y 200 se toman ahora por la capacidad actual de las computadoras. Con los algoritmos actuales de factorización y con las computadoras más potentes que existen puede tomar décadas factorizar un número de 200 cifras. Cuando se inventen máquinas capaces de factorizar números de 200 cifras en un tiempo razonable, estos valores se tendrán que incrementar, pero el método RSA seguirá funcionando sin problema.

Ahora describiremos cómo funciona el sistema RSA.

Supongamos que yo quiero tener un método seguro de recibir mensajes, por supuesto que esto también servirá para enviarlos, pero en ese caso, la persona que reciba los mensajes tiene que hacer lo que se va a describir.

Lo primero que tengo que hacer es encontrar dos números primos (o casi primos) p y q, de aproximadamente 100 cifras cada uno, al final de esta sección describimos cómo encontrar tales números. Los multiplicamos para obtener el número $m = p \cdot q$, el cual tiene aproximadamente 200 cifras. Como sabemos la factorización de m, seremos capaces de encontrar $\phi(m) = (p-1)(q-1)$ (ver Proposición 0.0.2). Éste es un punto importantísimo pues el número m se va a conocer públicamente como el número que yo uso para encriptar mensajes. Pero, como los demás no conocen su factorización, no podrán conocer el valor de $\phi(m)$.

Notemos que $\phi(m)$ es sólo un poco menor que m, pues para obtenerlo estamos multiplicando dos números ligeramente menores que p y q. Ahora nos escogemos un número k que satisfaga las siguientes condiciones: $0 < k < \phi(m)$ y $(k, \phi(m)) = 1$. Con el algoritmo de la división se puede encontrar tal k sin grandes problemas, y de una vez, aprovechando tal algoritmo, calculo el inverso de k módulo $\phi(m)$. Es decir, encuentro un número natural h tal que $kh \equiv 1 (\text{mod } \phi(m))$ *y* $h < m$. Finalmente doy a conocer a todos los interesados los números k y m y no importa en manos de quien caigan estos números. Esta información no es tan relevante como para que alguien sea capaz de decifrar un mensaje secreto que venga dirigido sólo a mí (a menos que alguien pudiera factorizar a m, lo cual es casi imposible).

Hasta este momento, todos conocen a k y a m, y mantengo en secreto los números p, q, h y $\phi(m)$.

Ahora supongamos que alguien está interesado en enviarme un mensaje. Como ya hemos dicho, esto es equivalente a enviarme una secuencia de números. Ya hemos dicho por qué no conviene enviar letra por letra (o su equivalente en números) pero se pueden enviar bloques de digamos 20 números cada uno. Más tarde veremos un ejemplo concreto de cómo descompondríamos un mensaje en números para enviarlo usando este método. De manera que el problema se reduce a saber cómo enviarme un número a que puede tener hasta unas 80 cifras. Observemos que con esto garantizamos que a no sea múltiplo ni de p ni de q y entonces a y m serán primos relativos.

Entonces, dado un número $a < m$, que me quiere enviar una persona en particular, lo que tiene que hacer es calcular el único número b tal que $0 \leq b < m$ y $b \equiv a^k (\text{mod } m)$. Y me envía el número b. No importa si el número b es interceptado por alguien pues sabiendo b no se puede conocer a a pues, la ecuación $b \equiv a^k (\text{mod } m)$ va a tener una única solución cuando se piensa que la incógnita es a y que se conoce b. Sin embargo, resolverla para a es bastante difícil, tal vez más difícil que factorizar m.

Finalmente, lo que yo tengo que hacer es encontrar el número c tal que $0 \leq c < m$ y $c \equiv b^h (\text{mod } m)$. A continuación haremos unas cuentas para comprobar que $a = c$, por lo que ya sabré el número que me enviaron.

Notemos que $(a, m) = 1$ por lo que $a^{\phi(m)} \equiv 1 (\text{mod } m)$. Por otra parte, sabemos que $kh \equiv 1 (\text{mod } \phi(m))$. De modo que existe un entero z positivo z tal que

$$kh = 1 + z\phi(m).$$

Puesto que

$$c \equiv b^h \equiv a^{kh} \equiv a^{1+z\phi(m)} \equiv a(a^{\phi(m)})^z \equiv a(1)^z \equiv a (\text{mod } m)$$

y

$$0 \leq c, a < m$$

concluimos que $a = c$.

EJEMPLO

Nada más para ilustrar, veremos un ejemplo numérico en el que aplicamos el método RSA.

Por supuesto que tenemos que tomar primos muy pequeños pues de lo contrario las cuentas se harían inmanejables en este texto. En la práctica no hay problema en manejar grandes números porque se usan las computadoras tanto para hacer las cuentas como para transmitir los mensajes.

Sean $p = 5$ y $q = 11$. Entonces $m = 55$ y $\phi(m) = 4 \cdot 10 = 40$. Ahora tenemos que escoger un número k que sea primo relativo con $\phi(m) = 40$. Como $40 = 2^3 \cdot 5$, cualquier número impar que no sea múltiplo de 5 servirá como k. Escogemos $k = 3$. De una vez calculamos el inverso de k módulo 40. Podríamos hacerlo usando el algoritmo de la división, pero en este caso sería una verdadera exageración ya que basta observar que $3 \cdot 27 = 81 \equiv 1 (\text{mod } 40)$ para saber que 27 es tal inverso. En nuestra notación $h = 27$.

En este momento, doy a conocer a k y m, y mantengo en secreto los números p, q, h y $\phi(m)$.

Supongamos que un amigo me quiere enviar la palabra CRIPTOGRAFÍA en forma cifrada. Usaremos la siguiente correspondencia entre las letras del alfabeto y los números del 0 al 55, la cual se obtiene de asignar a cada letra del alfabeto un número del sistema reducido de residuos módulo m (m=55)[1].

Texto Plano	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*
Ordinal	2	4	6	7	8	9	12	13	14

Texto Plano	*J*	*K*	*L*	*M*	*N*	$\tilde{N}$	*O*	*P*	*Q*
Ordinal	16	17	18	19	21	23	24	26	28

Texto Plano	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
Ordinal	29	31	32	34	36	37	38	39	41

[1]Un sistema reducido de residuos módulo m no es mas que el conjunto de números menores que m tal que cada número en el conjunto es primo relativo con m

Debemos notar que cada uno de estos numeros es primo relativo con 55. Entonces el mensaje se transforma en la secuencia de números:

$$6\ 29\ 14\ 26\ 32\ 24\ 12\ 29\ 2\ 9\ 14\ 2$$

En la práctica no se usa esta correspondencia. Se acostumbra a usar más el código ASCII (American Standard Code for Information Interchange) que le asigna a cada letra o símbolo un número de tres dígitos. Aquí transformamos letra por letra, ya dijimos que, en general esa no es una buena idea pero si aquí hacemos bloques nos van a salir números muy grandes, valga pues hacerlo así para este ejemplo.

De acuerdo con lo que explicamos antes mi amigo tiene que encontrar los números b tales que $a^k \equiv b(\text{mod } 55)$ y $0 < b < 55$, para cada uno de los números a que quiere transmitir, haciendo las cuentas pertinentes se obtiene que:

$6^3 \equiv 51(\text{mod } 55)$, $29^3 \equiv 24(\text{mod } 55)$, $14^3 \equiv 49(\text{mod } 55)$, $26^3 \equiv 31(\text{mod } 55)$, $32^3 \equiv 43(\text{mod } 55)$, $24^3 \equiv 19(\text{mod } 55)$, $12^3 \equiv 23(\text{mod } 55)$, $29^3 \equiv 24(\text{mod } 55)$, $2^3 \equiv 8(\text{mod } 55)$, $9^3 \equiv 14(\text{mod } 55)$, $14^3 \equiv 49(\text{mod } 55)$, $2^3 \equiv 8(\text{mod } 55)$

Entonces mi amigo me transmite la sequencia de números:

$$51\ 24\ 49\ 31\ 43\ 19\ 23\ 24\ 8\ 14\ 49\ 8$$

Para que yo sepa el mensaje transmitido tengo que encontrar los valores c tales que $b^h \equiv c(\text{mod } 55)$, donde b toma los valores que me fueron enviados, haciendo las cuentas pertinentes se obtiene que:

$$51^{27} \equiv 6(\text{mod } 55),\ 24^{27} \equiv 29(\text{mod } 55),\ 49^{27} \equiv 14(\text{mod } 55),$$
$$31^{27} \equiv 26(\text{mod } 55),\ 43^{27} \equiv 32(\text{mod } 55),\ 19^{27} \equiv 24(\text{mod } 55),$$
$$23^{27} \equiv 12(\text{mod } 55),\ 24^{27} \equiv 29(\text{mod } 55),\ 8^{27} \equiv 2(\text{mod } 55),$$
$$14^{27} \equiv 9(\text{mod } 55),\ 49^{27} \equiv 14(\text{mod } 55),\ 8^{27} \equiv 2(\text{mod } 55).$$

Entonces yo ya tengo la secuencia:

$$6\ 29\ 14\ 26\ 32\ 24\ 12\ 29\ 2\ 9\ 14\ 2$$

La cual puedo transformar otra vez en letras para, finalmente, obtener la palabra CRIPTOGRAFÍA.

En una primera lectura uno no capta la maravilla que es el método RSA. Observe usted que quien nos envía el mensaje no tiene que haber estado en contacto con nosotros antes, de hecho no tiene que conocernos y no tenemos que darle una clave secreta para que nos lo envíe. Lo único que tiene que saber esta persona es lo que sabe (o puede saber) todo el mundo, la k y la m. La idea de crear el RSA se ideó en dos partes. La idea de diseñar un sistema con estas características fue concebida por Whitfield Diffie en 1975. Quien lanzó al mundo matemático el reto de encontrar algunas funciones matemáticas específicas con las que se pudiera aterrizar esta idea. Él mismo junto con Hellman lo consiguieron en 1976 y en 1977 que Rivest, Shamir y Adleman se las ingeniaron para implementarlo en forma práctica.

Todos estos créditos que mencionamos en el párrafo anterior están bien otorgados, pero las personas mencionadas no fueron las primeras en diseñar este sistema. El inglés James Ellis hizo lo mismo que Diffie, es decir, concibió la idea de que hubiera un sistema de criptografía basado en una llave pública (la k y la m del método RSA) y una llave privada (las p, q, h y $\phi(m)$) para que cualquier persona me pudiera enviar un mensaje cifrado. Al igual que Diffie, Ellis sólo hizo el diseño teórico del sistema sin tener unas funciones matemáticas particulares que hicieran funcionar su método. El problema con Ellis es que trabajaba para la inteligencia británica en el GCHQ (Goverment Communications Headquarters) y todo su trabajo era clasificado como secreto y no se podía dar a conocer. Ellis concibió su idea en 1969 y les propuso a sus colegas la tarea de encontrar las funciones matemáticas que permitieran llevar a la práctica su idea, él mismo no era matemático. No fue sino hasta 1973 que el novato Clifford Cooks entró a trabajar a esta oficina, depués de trabajar ahí durante 6 semanas, su jefe, Nick Patterson, le platicó el problema que había propuesto Ellis y, en una tarde, Cooks lo resolvió inventando el metodo RSA. Por supuesto, los británicos no lo dieron a conocer y los norteamericanos lo redescubrieron como hemos platicado en el párrafo anterior.

La idea del RSA también se puede resumir en la siguiente forma. Si yo quiero recibir mensajes cifrados, doy a conocer una función $f : \{a \in \{0, 1, 2, ..., m-1\} : (a, m) = 1\} \to \{a \in \{0, 1, 2, ..., m-1\} : (a, m) = 1\}$, que

sea biyectiva. La función es $f(a) = b$, donde $b \equiv a^k (\text{mod } n)$. Como yo soy el único que conoce a f^{-1}, yo puedo saber quién es a.

Esto lo mencionamos porque, con el RSA y como la f puede ser conocida por cualquiera, entonces todo el mundo me puede mandar mensajes cifrados. Pero ¿cómo puedo tener certeza absoluta de que el mensaje es de una persona en particular? Bueno, pues también hay una manera de hacer esto. Para explicar cómo se hace, supongamos que quiero tener un intercambio de mensajes con la persona V y que ella da a conocer públicamente su función f_V, a mi función le llamo f_Y. Si yo recibo mensajes por medio de mi función f_Y, así nada más, no puedo estar seguro que vengan de V pues, mi línea de transmisión podría estar intervenida. Lo que podemos hacer V y Yo, es convenir en una palabra clave que vaya acompañada de la fecha del mensaje. Podrá usted decir, que si podemos convenir una palabra clave y secreta, entonces no necesitamos de estarnos mandando mensajes cifrados pues, por la misma vía en que nos dijimos la palabra secreta (podría haber sido personalmente), nos podríamos estar diciendo lo que quisiéramos. Tiene usted razón pero la ventaja de lo de la palabra clave es que sólo la tenemos que decir una vez y, después podemos mandarnos muchos mensajes en forma secreta y a distancia. Bueno pues para no hacerlo más largo, supongamos que la palabra clave junto con la fecha del mensaje del día está representada por el número a. Entonces, en todos los mensajes V podría empezar enviando la "palabra" $f_Y(f_V^{-1}(a))$. Entonces yo le puedo aplicar $f_V(f_Y^{-1}(f_Y(f_V^{-1}(a)))) = a$. Por supuesto que yo conozco f_Y^{-1} y f_V (pues esta última es pública). Y al reconocer yo la palabra clave y la fecha puedo estar seguro que V me está enviando el mensaje, pues V es la única persona que pudo haberlo enviado pues es la única que conoce a f_V^{-1}. Ésta es una manera de "firmar" mensajes cifrados.

En este momento uno se puede preguntar si hay algunas otras funciones matemáticas que sirvan para el mismo objetivo y la respuesta es sí. En las siguientes secciones desarrollaremos los conceptos de curvas elípticas y veremos cómo pueden ser usadas para encriptar mensajes en forma similar a la que se hizo para el RSA. El hecho de buscar otras maneras diferentes de implementar este sistema de encriptado no se debe sólo a la curiosidad de los matemáticos sino también a una razón práctica muy concreta. ¿Qué tal que se descubre algún método fabuloso para factorizar números naturales que haga inútil al RSA? Ya hasta ha habido películas en las que el protagonista

hace este descubrimiento e imagínese lo que se puede hacer con semejante paquete. En la actualidad el RSA es usado por gobiernos, bancos, empresas, etc.

En principio, el RSA funciona de maravilla si tenemos dos primos p y q. Pero como podría usted sospechar, no es tan fácil encontrarse dos primotes de 100 cifras. Pensemos un poco cómo encontrar un primo de ese tamaño. Si tomamos un número z de 100 cifras, si no tenemos más herramientas, para determinar si es primo o no, tenemos que buscar si se puede factorizar o no. Observe que esto es lo que no se puede hacer razonablemente para números de 200 cifras y por eso el RSA funciona. Pues resulta que tampoco es fácil hacerlo para números de 100 cifras y entonces se tienen que buscar métodos alternativos. Una buena forma de ver si un número es casi primo es usar el Pequeño Teorema de Fermat. Recuerde que este resultado dice que, si $(a, z) = 1$ y z es primo, entonces $a^{z-1} \equiv 1 (\text{mod } z)$. De manera que, si existe una $a < z$ tal que a^{z-1} no es congruente a 1 módulo z, entonces z no es primo. Lo que se hace en la práctica, es tomar z, tomar varios números a tales que $1 < a < z$ y verificar si ocurre la congruencia $a^{z-1} \equiv 1 (\text{mod } z)$, entre más números a sean revisados podemos estar más confiados (aunque nunca podremos estar completamente seguros) de que z es primo. Se ha mostrado que la probabilidad de que z no sea primo cuando tomamos un número adecuado de números a es muy baja y entonces el método RSA se trabaja con estos números z que se acercan mucho a los primos. Por supuesto que hay otros métodos para obtener números que son casi primos que son razonablemente confiables y accesibles pero que necesitan de más teoría. Sin embargo, el que hemos descrito, basado en el Pequeño Teorema de Fermat, es bastante bueno.

2.7. MÉTODO MASSEY-OMURA

Otro de los grandes problemas dentro de la teoría de números es el llamado Problema del Logaritmo Discreto. Este problema consiste en calcular x a partir de la expresión $y \equiv a^x \pmod{p}$, donde p es un número cualquiera, a e y son números enteros.

En principio, una forma de resolver este problema sería calcular $a^t \pmod{p}$ para todo t entre 1 y p. Si logramos encontrar entre estos enteros un entero

t_0 tal que $y \equiv a^{t_0} \pmod{p}$, entonces hacemos $x = t_0$ y así encontramos el valor de x.

Este proceso resulta muy sencillo de seguir, pero resulta demasiado extenso cuando p es un número muy grande, digamos por ejemplo un número que tuviera 200 cifras, puede imaginarse lo complicado que sería repetir el proceso anterior 10^{200} veces aproximadamente.

Basados en este problema tenemos los métodos Massey-Omura y ElGamal, empezaremos por describir el Massey-Omura.

Descripción

Supongamos que un grupo de personas desean enviar y recibir mensajes entre ellos. El Primer paso será que de común acuerdo, escojan un número primo q lo suficientemente grande. A continuación deberán escoger el tamaño de los bloques que serán utilizados para dividir los textos. Posteriormente deberán asignar un número a cada uno de los posibles bloques que puedan obtenerse, de tal manera que si se tienen 2 posibles bloques distintos entonces éstos tengan asignados 2 números distintos. Además deberán cuidar que cada número asignado a un bloque sea primo relativo con q, es decir, si k es un número asignado a un bloque entonces $(k, q) = 1$.

El número q, así como también la información de cuáles son los bloques que se pueden utilizar y el número que tiene asignado cada bloque se hacen del conocimiento de todas los miembros del grupo, inclusive pueden ser conocidos por personas ajenas al grupo sin que se comprometa la seguridad.

A continuación cada persona deberá elegir un número el cual sea primo relativo con $q - 1$, es decir, cada persona elegirá un número e tal que $(e, q - 1) = 1$. Una vez elegido e deberá calcular su inverso multiplicativo módulo $q - 1$, de tal manera que encontrará un número d tal que:

$$de \equiv 1 \pmod{q - 1}$$

cada persona mantendrá en secreto sus números e y d.

El siguiente paso será el envío y recepción de mensajes. Cabe resaltar que en este método a diferencia de otros no quedan separados claramente los procesos de encriptación y desencriptacíon. En los métodos hasta ahora

analizados sólo se hace un envío de la información encriptada y la persona que recibe la información debera desencriptarla. Sin embargo como se vera a continuación el método Massey-Omura tiene la particularidad de que se hace un envío repetido de información, por lo que, se hace una encriptación repetida de la misma. Más precisamente la información es encriptada y enviada 3 veces y en la cuarta encriptación se da también la desencriptación de la información.

Para describir cómo se hará el envío de la información tomaremos a dos personas del grupo de personas que mencionamos al principio, las cuales denotaremos con las letras A y B. Estas personas desean enviarse y recibir mensajes entre ellas, lo hacemos de esta manera por simplicidad pero podemos extenderlo a un número mayor de personas. Tanto A como B cuentan con una pareja de números enteros de la forma (e, d), pongamos (e_A, d_A) para A y (e_B, d_B) para B.

Ahora bien supongamos que la persona A desea enviarle un mensaje a la persona B. Para ello primeramente deberá dividir el mensaje que desea enviar en bloques del tamaño elegido previamente y cambiar cada bloque por el número que le corresponda según la asignación que acordaron al principio las personas del grupo. Al hacer A este cambio obtendrá una serie de números, digamos que la serie que obtuvo fue $w_0, w_1, \ldots, w_m$. El siguiente paso será mandarle esta información a B, pero necesita mandársela encriptada, ya que de enviar esta información sin encriptar, como las demás personas del grupo conocen qué bloque de texto le corresponde a cada número entonces podrán leer el mensaje lo cual no desea A.

Para encriptar el mensaje la persona A tomará cada número de la serie $w_0, w_1, \ldots, w_m$ y lo multiplicará por sí mismo e_A veces calculando cada resultado módulo q. De tal manera que por cada número w_i con $0 \leqslant i \leqslant m$ obtendrá un valor x_i tal que

$$x_i \equiv (w_i)^{e_A} \pmod{q}$$

por lo que podrá formar una nueva serie la cual será $x_0, x_1, \ldots, x_m$. Esta serie será la que enviará a la persona B.

La persona B al recibir la serie $x_0, x_1, \ldots, x_m$, no podrá descifrar el mensaje, ya que para ello debería calcular $(x_i)^{-e_A}$ (este calculó se realiza *mod* q

por lo que obtendremos un número entero) esto para $0 \leqslant i \leqslant m$, esto debido a que como $x_i \equiv (w_i)^{e_A} \pmod{q}$ entonces obtendría

$$(x_i)^{-e_A} = \left((w_i)^{e_A}\right)^{-e_A} \equiv w_i \pmod{q}$$

con lo cual podría encontrar los números correspondientes a cada bloque del texto que le envío A. Pero como e_A es un número secreto de A entonces es desconocido por B, por lo que B no podrá realizar el calculo de $(x_i)^{-e_A}$. Sin embargo la persona B puede encriptar la serie que recibió y enviarle la serie que obtenga a A. La persona B lo que hará será tomar cada número de la serie que le envió A, multiplicar este número e_B veces y hacer el cálculo modulo q, es decir, para cada entero i que se encuentre entre 0 y m buscará el número y_i mediante la siguiente fórmula

$$y_i \equiv (x_i)^{e_B} \pmod{q}$$

al hacer este proceso para cada i, la persona B obtendrá la serie $y_0, y_1, \ldots, y_m$, la cual enviará a A.

La persona A como ya conoce el mensaje no le interesa desencriptar la información que le envío B, por lo que simplemente vuelve a encriptar la serie que recibe de B y se la envía. Para hacer esto la persona A lo que hace es multiplicar cada término de la serie por sí mismo un número d_A de veces y hacer el cálculo módulo q. Así por cada entero i entre 0 y m encontrará un número z_i tal que:

$$z_i \equiv (y_i)^{d_A} \pmod{q}$$

con los que formará la serie $z_0, z_1, \ldots, z_m$, la cual enviará a la persona B. Debemos mencionar algo importante, debido a que para cada i tenemos que $y_i \equiv (x_i)^{e_B} \pmod{q}$ y $x_i \equiv (w_i)^{e_A} \pmod{q}$ entonces tendremos que

$$z_i \equiv (y_i)^{d_A} \equiv \left((x_i)^{e_B}\right)^{d_A} \equiv \left(\left((w_i)^{e_A}\right)^{e_B}\right)^{d_A} \pmod{q}$$

pero si recordamos la persona A calculó d_A de tal forma que

$$d_A \equiv (e_A)^{-1} \pmod{q-1},$$

por lo que $d_A e_A \equiv 1 \pmod{q-1}$. Esto quiere decir que existe un número b tal que $d_A e_A - 1 = b(q-1)$ y entonces $d_A e_A = 1 + b(q-1)$ por lo que

$$\begin{aligned} z_i &\equiv (y_i)^{d_A} \equiv \left(\left((w_i)^{e_A}\right)^{e_B}\right)^{d_A} \equiv \left((w_i)^{e_B}\right)^{e_A d_A} \\ &\equiv \left((w_i)^{e_B}\right)^{1+b(q-1)} \equiv \left((w_i)^{e_B}\right)^{1}\left((w_i)^{e_B}\right)^{b(q-1)} (\text{mod } q) \end{aligned}$$

Ahora bien debido a que como q es un número primo entonces por la definición de la función ϕ de Euler tendremos que $\phi(q) = q - 1$. Además de esto como cada w_i es un número que fue asignado a un bloque, entonces se tendrá que $(w_i, q) = 1$. De lo anterior por el Corolario 4 del apéndice A tendremos que $(w_i)^{q-1} = (w_i)^{\phi(q)} \equiv 1 \pmod{q}$. De esto obtendremos que

$$\begin{aligned} z_i &\equiv \left((w_i)^{e_B}\right)^{1}\left((w_i)^{e_B}\right)^{b(q-1)} \equiv (w_i)^{e_B}\left((w_i)^{q-1}\right)^{be_B} \\ &\equiv (w_i)^{e_B}(1)^{be_B} \equiv (w_i)^{e_B} (\text{mod } q) \end{aligned}$$

Esta información que acabamos de obtener le será de gran ayuda a la persona B cuando recibe la serie $z_0, z_1, \ldots, z_m$ ya que, si él calcula para cada i:

$$(z_i)^{d_B} \pmod{q}$$

sabe que encontrara los números correspondientes a cada bloque del texto que quería enviarle A, ya que por los últimos cálculos tendremos que

$$(z_i)^{d_B} \equiv \left({w_i}^{e_B}\right)^{d_B} \equiv {w_i}^{e_B d_B} (\text{mod } q)$$

y como $e_B d_B \equiv 1 \pmod{q-1}$ entonces existe un número r en los enteros tal que $r(q-1) = e_B d_B - 1$, de lo cual $e_B d_B = r(q-1) + 1$ y nuevamente por el Corolario 4 del apéndice A tendremos que

$$(z_i)^{d_B} \equiv {w_i}^{e_B d_B} \equiv {w_i}^{r(q-1)+1} \equiv {w_i}^{r(q-1)} * {w_i}^{1} \equiv w_i \pmod{q}$$

Debido a esto si para cada i la persona B calcula $(z_i)^{d_B} \pmod{q}$, entonces obtendrá la serie $w_0, w_1, \ldots, w_m$ y una vez obtenida esta serie entonces podrá encontrar el texto que le envió la persona A.

A continuación haremos un pequeño ejemplo, el cual sólo será ilustrativo. En este ejemplo el tamaño de los bloques que utilizaremos será 1, de tal

manera que la separación del texto estará hecha por las letras del alfabeto. Para no hacer demasiado largas las cuentas utilizaremos como q al número 83 y haremos la siguiente asignación entre las letras del alfabeto y algunos números primos relativos con 82, debido a que en el método se requiere que cada valor asignado a un bloque sea primo relativo con $q-1$. Notemos que los divisores de 82 son 2 y 41, por lo que debemos elegir números que no sean multiplos de 2 o de 41.

Texto Plano	A	B	C	D	E	F	G	H	I
Ordinal	1	3	5	7	9	11	13	21	23

Texto Plano	J	K	L	M	N	$\tilde{N}$	O	P	Q
Ordinal	25	27	29	31	33	35	37	39	43

Texto Plano	R	S	T	U	V	W	X	Y	Z
Ordinal	45	47	49	51	53	55	57	59	61

Una vez hecho lo anterior supongamos que la persona A ha escogido $e_A = 9$ y que la persona B escogió $e_B = 13$. Entonces tendremos que $d_A = 52$ y $d_B = 32$. Supongamos que la persona A desea enviar la palabra ENCRIPTACION a la persona B, nota que a esta palabra le corresponde la serie

$$9,\ 33,\ 5,\ 45,\ 23,\ 39,\ 49,\ 1,\ 5,\ 23,\ 37,\ 33$$

entonces la persona A al elevar cada uno de estos números a la octava potencia (porque $a_B = 8$) y calcular el resultado módulo 83 obtendrá:

$$9^9 \equiv 61 (\text{mod } 83),\ 33^9 \equiv 75 (\text{mod } 83),\ 5^9 \equiv 52 (\text{mod } 83),\ 45^9 \equiv 18 (\text{mod } 83),$$
$$23^9 \equiv 38 (\text{mod } 83),\ 39^9 \equiv 20 (\text{mod } 83),\ 49^9 \equiv 9 (\text{mod } 83),\ 1^9 \equiv 1 (\text{mod } 83),$$
$$5^9 \equiv 52 (\text{mod } 83),\ 23^9 \equiv 38 (\text{mod } 83),\ 37^9 \equiv 49 (\text{mod } 83),\ 33^9 \equiv 75 (\text{mod } 83).$$

por lo que tendrá la serie

$$61,\ 75,\ 52,\ 18,\ 38,\ 20,\ 9,\ 1,\ 52,\ 38,\ 49,\ 75$$

la cual le enviará a B. La persona B tomará cada elemento de esta serie y entonces lo elevará a la potencia 13, que corresponde a su número e_B y calculará el resultado módulo q con lo cual obtendrá:

$$61^{13} \equiv 31(\text{mod } 83),\ 75^{13} \equiv 21(\text{mod } 83),\ 52^{13} \equiv 79(\text{mod } 83),$$
$$18^{13} \equiv 42(\text{mod } 83),\ 38^{13} \equiv 69(\text{mod } 83),\ 20^{13} \equiv 76(\text{mod } 83),$$
$$9^{13} \equiv 78(\text{mod } 83),\ 1^{13} \equiv 1(\text{mod } 83),\ 52^{13} \equiv 79(\text{mod } 83),$$
$$38^{13} \equiv 69(\text{mod } 83),\ 49^{13} \equiv 75(\text{mod } 83),\ 75^{13} \equiv 21(\text{mod } 83).$$

Así la serie que enviará a la persona A será

$$31,\ 21,\ 79,\ 42,\ 69,\ 76,\ 78,\ 1,\ 79,\ 69,\ 75,\ 21$$

De donde A, al recibirlos, multiplicará cada uno de estos valores por sí mismos tantas veces como d_A (es decir, 11) y calculará el resultado módulo q, obteniendo así:

$$31^{73} \equiv 78(\text{mod } 83),\ 21^{73} \equiv 30(\text{mod } 83),\ 79^{73} \equiv 47(\text{mod } 83),$$
$$42^{73} \equiv 14(\text{mod } 83),\ 69^{73} \equiv 81(\text{mod } 83),\ 76^{73} \equiv 55(\text{mod } 83),$$
$$78^{73} \equiv 75(\text{mod } 83),\ 1^{73} \equiv 1(\text{mod } 83),\ 79^{73} \equiv 47(\text{mod } 83),$$
$$69^{73} \equiv 81(\text{mod } 83),\ 75^{73} \equiv 33(\text{mod } 83),\ 21^{73} \equiv 30(\text{mod } 83).$$

por lo que A le enviará a B la serie

$$78,\ 30,\ 47,\ 14,\ 81,\ 55,\ 75,\ 1,\ 47,\ 81,\ 33,\ 30$$

Así finalmente B hará lo siguiente

$$78^{9} \equiv 9(\text{mod } 83),\ 30^{19} \equiv 33(\text{mod } 83),\ 47^{19} \equiv 5(\text{mod } 83),$$
$$14^{19} \equiv 45(\text{mod } 83),\ 81^{19} \equiv 23(\text{mod } 83),\ 55^{19} \equiv 39(\text{mod } 83),$$
$$75^{19} \equiv 49(\text{mod } 83),\ 1^{19} \equiv 1(\text{mod } 83),\ 47^{19} \equiv 5(\text{mod } 83),$$
$$81^{19} \equiv 23(\text{mod } 83),\ 33^{19} \equiv 37(\text{mod } 83),\ 30^{19} \equiv 33(\text{mod } 83).$$

de donde obtendrá la serie

$$9,\ 33,\ 5,\ 45,\ 23,\ 39,\ 49,\ 1,\ 5,\ 23,\ 37,\ 33$$

de donde puede deducir que el mensaje que le envío A es ENCRIPTACION. Debemos mencionar que la persona A no necesariamente tiene que hacer la encriptación primero con e_A y después con d_A sino que puede utilizar primero d_A y despues e_A ya que al final de cuentas se obtendrán los mismos resultados. Análogamente, B en lugar de utilizar primero e_B y después d_B, puede usar primero d_B y a continuación e_B.

2.8. MÉTODO ELGAMAL

Al igual que en el método anterior, supondremos que un grupo de personas desea enviar y recibir mensajes entre ellos, y que ya han decidido de qué tamaño serán los bloques que utilizarán, así como también, ya habrán hecho la asignación de un número a cada bloque. Además de lo anterior deberán elegir un número p que sea primo y un número g el cual cumpla que $1 \leqslant g \leqslant p-1$. Tanto p como g deberán hacerse públicos.

Una vez que todos conocen esta información cada persona elegirá un número a el cual no sea divisible por p y debera calcular $g^a \pmod{p}$, el valor resultante de esta operación será su llave pública y el número a será su llave privada, es decir, cada persona contará con un pareja de números (a, b), en donde $b \equiv g^a \pmod{p}$ es conocido por cualquier persona que lo desee y a es un número que solo él conocerá.

Encriptación

El siguiente paso será el envío de mensajes, para ello tomaremos a 2 personas a las que llamaremos A y B, las cuales cuentan con las parejas $(a_A,\ b_A)$ y $(a_B,\ b_B)$ respectivamente, debemos recalcar que como b_A y b_B son públicos entonces A conoce b_B y B conoce b_A. Supongamos que A desea enviarle un mensaje a B para lo cual ya ha dividido el texto en bloques y ya cambió cada bloque por el número respectivo, obteniendo así una serie de números $n_1, n_2, \ldots, n_m$. Con esto la persona A, como conoce b_B calculará $b_B^{a_A} \pmod{p}$ de donde obtendrá un valor c.

Una vez que A ha calculado c multiplicará este valor por cada uno de los números de la serie $n_1, n_2, \ldots, n_m$. Al hacer cada una de estas multiplicaciones deberá calcular el resultado módulo p, es decir, para cada n_i con $1 \leqslant i \leqslant m$ buscará un valor q_i tal que

$$q_i \equiv n_i c \pmod{p}$$

Una vez calculados todos los q_i, entonces enviará a B la serie

$$q_1, q_2, \ldots, q_m$$

y con esto concluirá el proceso de encriptación.

Desencriptación

El siguiente paso será desencriptar el mensaje, proceso que queda a cargo de la persona B, para ello cuenta con la siguiente información

1	$q_1, q_2, \ldots, q_m$	Mensaje cifrado
2	a_B	Llave privada de B
3	b_A	Llave pública de A

con esta información, lo que hará B para poder encontrar el mensaje que le envío A será primero calcular $b_A^{a_B} \pmod p$, de lo cual obtendrá un valor x. Cabe resaltar que como $b_A \equiv g^{a_A} \pmod p$, entonces $x \equiv (b_A)^{a_B} \equiv (g^{a_A})^{a_B} \pmod p$. Una vez que B ha encontrado x entonces buscará un número z tal que $z \equiv (x)^{-1} \pmod q$. A este número z deberá multiplicarlo por cada uno de los números q_i $(1 \leqslant i \leqslant m)$ que le envío A. El resultado de cada una de estas multiplicaciones deberá calcularlo módulo p, es decir,

$$zq_i \pmod q, \quad \text{con} \quad 1 \leqslant i \leqslant m$$

al realizar los cálculos anteriores B encontrará que, como $z \equiv x^{-1} \pmod p$ y $q_i \equiv n_i c \pmod p$, entonces

$$zq_i \equiv (x^{-1})n_i c \pmod p$$

pero $c \equiv b_B^{a_A} \pmod p$, por lo que

$$zq_i \equiv (x^{-1})n_i c \equiv (x^{-1})n_i(b_B^{a_A}) \pmod p$$

y debido a que $x \equiv b_A^{a_B} \pmod p$ entonces

$$zq_i \equiv (b_A^{a_B})^{-1}n_i(b_B^{a_A}) \pmod p$$

finalmente recordemos que $b_A \equiv g^{a_A} \pmod p$ y $b_B \equiv g^{a_B} \pmod p$, entonces para zq_i tendremos

$$\begin{aligned} zq_i &\equiv (b_A^{a_B})^{-1}n_i(b_B^{a_A}) \equiv \Big((g^{a_A})^{a_B}\Big)^{-1} n_i \Big((g^{a_B})^{a_A}\Big) \\ &\equiv n_i \Big((g^{a_A})^{a_B}\Big)^{-1} \Big((g^{a_B})^{a_A}\Big) \equiv n_i \pmod p \end{aligned}$$

Con esto la persona B podrá reconocer a cada una de las q_i de tal manera que podrá recuperar la serie $q_1, q_2, \ldots q_m$ y con ello recuperar el mensaje que le enviará A. Con lo cual terminamos la descripción del método.

Ejemplo

Como ejemplo utilizaremos a dos personas a las que llamaremos A y B las cuales han decidido que sus mensajes no los mandarán letra por letra sino que dividirán sus textos en parejas de letras. Como la persona A desea enviar a B la palabra ENCRIPTACION NUMERICA, entonces deberá dividir la palabra de la siguiente manera EN-CR-IP-TA-CI-ON-*N-UM-ER-IC-A*, aquí el símbolo $*$ lo estamos ocupando para los espacios en blanco. El siguiente problema que deberán resolver es cómo asignar un número a cada bloque posible, para ello han construido una tabla, la cual se muestra al final de la sección.

El proceso para contruir la tabla es el siguiente, digamos que queremos encontrar el número que le corresponde al bloque UX, entonces buscamos que número le corresponde a U y a X en la siguiente tabla.

Texto Plano	A	B	C	D	E	F	G	H	I	J
Ordinal	1	2	3	4	5	6	7	8	9	10

Texto Plano	K	L	M	N	$\tilde{N}$	O	P	Q	R
Ordinal	11	12	13	14	15	16	17	18	19

Texto Plano	S	T	U	V	W	X	Y	Z	$*$
Ordinal	20	21	22	23	24	25	26	27	28

como el número que le corresponde a U es 22 y el de X es 25 entonces calculan $(22-1)*28+25 = 588+25 = 613$ y este es el número que le corresponde al bloque UX. Más precisamente, si en un bloque la primer letra tiene asignado el número a y la segunda letra el número b, entonces el número asignado a tal bloque será $(a-1)*28+b$.

Debido a lo anterior los números asignados a EN-CR-IP-TA-CI-ON-*N-UM-ER-IC-A* podrán ser calculados como sigue:

Bloque	Número de la primera letra	Número de la segunda letra		Operación		Número asignado al bloque
??	x	y		$(x-1)28+y=z$		c
EN	5	14		(5-1)*28+14=112+14=127		127
CR	3	19		(3-1)*28+19=56+19=75		75
IP	9	17		(9-1)*28+17=224+17=241		241
TA	21	1		(21-1)*28+1=560+1=561		561
CI	3	9		(3-1)*28+9=56+9=65		65
ON	16	14		(16-1)*28+14=420+14=434		434
*N	28	14		(28-1)*28+14=756+14=470		470
UM	22	13		(22-1)*28+13=588+13=601		601
ER	5	19		(5-1)*28+19=112+19=131		131
IC	9	3		(9-1)*28+3=224+3=227		227
A*	1	28		(1-1)*28+28=0+28=28		28

por lo que el texto ENCRIPTACION NUMERICA tendrá asignada la serie

$$127,\ 75,\ 241,\ 561,\ 65,\ 434,\ 470,\ 601, 131,\ 227,\ 28$$

Por otro lado han elegido de común acuerdo que $p = 787$ y $g = 29$, además cada uno ha elegido su número secreto y su número público, y este último ya se lo han hecho llegar a la otra persona. En el caso de A ha elegido $a_A = 13$, por lo que $b_A = g^{a_A} = 29^{13} = 10260628712958602189 \equiv 734 \pmod{787}$. Y B ha escogido $a_B = 11$, y a partir de este número ha calculado g^{a_B} lo cual le ha dado como resultado $b_B = 29^{11} = 12200509765705829 \equiv 684 \pmod{787}$. De tal manera que la pareja de números de A es $(13, 734)$ y la de B es $(11, 684)$.

Como el mensaje que desea enviarle A a B es ENCRIPTACION NUMERICA el cual tiene asignado la serie

$$127,\ 75,\ 241,\ 561,\ 65,\ 434,\ 470,\ 601,\ 31,\ 227,\ 28$$

deberá calcular primero $b_B^{a_A} \pmod{787}$, es decir, $(684)^{13} \equiv 420 \pmod{787}$ de donde el número c que aparece en la descripción del método es 420. Recordemos que este cálculo lo puede hacer ya que $b_B = 684$ es el número público de B por lo que lo conoce A. Una vez que ha calculado el número

c la persona A deberá multiplicar este número por cada número de la serie que corresponde al texto que desea enviar a B, de tal manera que hará los siguientes cálculos.

$$\begin{gathered}420(127) \equiv 611 \pmod{787},\ \ 420(75) \equiv 20 \pmod{787},\\ 420(241) \equiv 484 \pmod{787},\ 420(561) \equiv 307 \pmod{787},\\ 420(65) \equiv 542 \pmod{787},\ \ 420(434) \equiv 483 \pmod{787},\\ 420(470) \equiv 650 \pmod{787},\ \ 420(601) \equiv 580 \pmod{787},\\ 420(31) \equiv 428 \pmod{787},\ \ 420(227) \equiv 113 \pmod{787},\\ 420(28) \equiv 742 \pmod{721},\end{gathered}$$

de donde obtendrá la serie

$$611,\ 20,\ 484,\ 307,\ 542,\ 483,\ 650,\ 580,\ 428,\ 113,\ 742$$

la cual enviará a B. Una vez que B recibe esta serie de números debera calcular $x = (b_A)^{a_B} \pmod{787}$, este cálculo lo puede hacer ya que sabe quien es b_A porque este número ya lo hizo público A. Entonces B encontrará que

$$x = (734)^{11} = 333162919448963652411872231075 84 \equiv 420 \pmod{787}$$

así, una vez que B sabe que $x = 420$ entonces calcula el inverso multiplicativo de este número y el resultado lo calcula módulo 787, con esto encontrará un valor z tal que $z = b_A^{a_B} \equiv 594 \pmod{787}$. De acuerdo a la descripción que se hizo del método este número z que encontró B deberá multiplicarlo por cada uno de los números que le envío A y calcular el resultado módulo 787. Con esto podrá encontrar algunos números que verificará en la tabla al final de la sección para ver a que bloques pertenecen y así poder encontrar el mensaje que le envío A. El resultado de las operaciones es el siguiente:

$$\begin{gathered}594(611) \equiv 127 \pmod{787},\ \ 594(20) \equiv 75 \pmod{787},\\ 594(484) \equiv 241 \pmod{787},\ 594(307) \equiv 561 \pmod{787},\\ 594(542) \equiv 65 \pmod{787},\ \ 594(483) \equiv 434 \pmod{787},\\ 594(650) \equiv 470 \pmod{787},\ \ 594(580) \equiv 601 \pmod{787},\\ 594(428) \equiv 31 \pmod{787},\ \ 594(113) \equiv 227 \pmod{787},\\ 594(742) \equiv 28 \pmod{721},\end{gathered}$$

De donde B obtendrá la serie

$$127,\ 75,\ 241,\ 561,\ 65,\ 434,\ 470,\ 601,\ 31,\ 227,\ 28$$

que corresponde al texto ENCRIPTACION NUMERICA, con esto habrá llegado el mensaje a su destinatario.

Tabla

Bloque	Número
AA	1
AD	4
AG	7
AJ	10
AM	13
AO	16
AR	19
AU	22
AX	25
A*	28
BC	31
BF	34
BI	37
BL	40
BÑ	43
BQ	46
BT	49
BW	52
BZ	55
CB	58
CE	61
CH	64
CK	67
CN	70
CP	73
CS	76
CV	79
CY	82
DA	85
DD	88
DG	91
DJ	94
DM	97
DO	100

Bloque	Número
AB	2
AE	5
AH	8
AK	11
AN	14
AÑ	15
AQ	18
AT	21
AV	23
AY	26
BA	29
BD	32
BG	35
BJ	38
BM	41
BO	44
BR	47
BU	50
BX	53
B*	56
CC	59
CF	62
CI	65
CL	68
CÑ	71
CQ	74
CT	77
CW	80
CZ	83
DB	86
DE	89
DH	92
DK	95
DN	98
DP	101

Bloque	Número
AC	3
AF	6
AI	9
AL	12
AÑ	15
AQ	18
AT	21
AW	24
AZ	27
BB	30
BE	33
BH	36
BK	39
BN	42
BP	45
BS	48
BV	51
BY	54
CA	57
CD	60
CG	63
CJ	66
CM	69
CO	72
CR	75
CU	78
CX	81
C*	84
DC	87
DF	90
DI	93
DL	96
DÑ	99
DQ	102

Tabla

Bloque	Número
DR	103
DU	106
DX	109
D*	112
EC	115
EF	118
EI	121
EL	124
EÑ	127
EQ	130
ET	133
EW	136
EZ	139
FB	142
FE	145
FH	148
FK	151
FN	154
FP	157
FS	160
FV	163
FY	166
GA	169
GD	172
GG	175
GJ	178
GM	181
GO	184
GR	187
GU	190
GX	193
G*	196
HC	199
HF	202

Bloque	Número
DS	104
DV	107
DY	110
EA	113
ED	116
EG	119
EJ	122
EM	125
EO	128
ER	131
EU	134
EX	137
E*	140
FC	143
FF	146
FI	149
FL	152
FÑ	155
FQ	158
FT	161
FW	164
FZ	167
GB	170
GE	173
GH	176
GK	179
GN	182
GP	185
GS	188
GV	191
GY	194
HA	197
HD	200
HG	203

Bloque	Número
DT	105
DW	108
DZ	111
EB	114
EE	117
EH	120
EK	123
EN	126
EP	129
ES	132
EV	135
EY	138
FA	141
FD	144
FG	147
FJ	150
FM	153
FO	156
FR	159
FU	162
FX	165
F*	168
GC	171
GF	174
GI	177
GL	180
GÑ	183
GQ	186
GT	189
GW	192
GZ	195
HB	198
HE	201
HH	204

Tabla

Bloque	Número
HI	205
HL	208
HÑ	211
HQ	214
HT	217
HW	220
HZ	223
IB	226
IE	229
IH	232
IK	235
IN	238
IP	241
IS	244
IV	247
IY	250
JA	253
JD	256
JG	259
JJ	262
JM	265
JO	268
JR	271
JU	274
JX	277
J*	280
KC	283
KF	286
KI	289
KL	292
KÑ	295
KQ	298
KT	301
KW	304

Bloque	Número
HJ	206
HM	209
HO	212
HR	215
HU	218
HX	221
H*	224
IC	227
IF	230
II	233
IL	236
IÑ	239
IQ	242
IT	245
IW	248
IZ	251
JB	254
JE	257
JH	260
JK	263
JN	266
JP	269
JS	272
JV	275
JY	278
KA	281
KD	284
KG	287
KJ	290
KM	293
KO	296
KR	299
KU	302
KX	305

Bloque	Número
HK	207
HN	210
HP	213
HS	216
HV	219
HY	222
IA	225
ID	228
IG	231
IJ	234
IM	237
IO	240
IR	243
IU	246
IX	249
I*	252
JC	255
JF	258
JI	261
JL	264
JÑ	267
JQ	270
JT	273
JW	276
JZ	279
KB	282
KE	285
KH	288
KK	291
KN	294
KP	297
KS	300
KV	303
KY	306

Tabla

Bloque	Número
KZ	307
LB	310
LE	313
LH	316
LK	319
LN	322
LP	325
LS	328
LV	331
LY	334
MA	337
MD	340
MG	343
MJ	346
MM	349
MO	352
MR	355
MU	358
MX	361
M*	364
NC	367
NF	370
NI	373
NL	376
NÑ	379
NQ	382
NT	385
NW	388
NZ	391
ÑB	394
ÑE	397
ÑH	400
ÑK	403
ÑN	406

Bloque	Número
K*	308
LC	311
LF	314
LI	317
LL	320
LÑ	323
LQ	326
LT	329
LW	332
LZ	335
MB	338
ME	341
MH	344
MK	347
MN	350
MP	353
MS	356
MV	359
MY	362
NA	365
ND	368
NG	371
NJ	374
NM	377
NO	380
NR	383
NU	386
NX	389
N*	392
ÑC	395
ÑF	398
ÑI	401
ÑL	404
ÑÑ	407

Bloque	Número
LA	309
LD	312
LG	315
LJ	318
LM	321
LO	324
LR	327
LU	330
LX	333
L*	336
MC	339
MF	342
MI	345
ML	348
MÑ	351
MQ	354
MT	357
MW	360
MZ	363
NB	366
NE	369
NH	372
NK	375
NN	378
NP	381
NS	384
NV	387
NY	390
ÑA	393
ÑD	396
ÑG	399
ÑJ	402
ÑM	405
ÑO	408

Tabla

Bloque	Número	Bloque	Número	Bloque	Número
ÑP	409	**ÑQ**	410	**ÑR**	411
ÑS	412	**ÑT**	413	**ÑU**	414
ÑV	415	**ÑW**	416	**ÑX**	417
ÑY	418	**ÑZ**	419	**Ñ***	420
OA	421	**OB**	422	**OC**	423
OD	424	**OE**	425	**OF**	426
OG	427	**OH**	428	**OI**	429
OJ	430	**OK**	431	**OL**	432
OM	433	**ON**	434	**OÑ**	435
OO	436	**OP**	437	**OQ**	438
OR	439	**OS**	440	**OT**	441
OU	442	**OV**	443	**OW**	444
OX	445	**OY**	446	**OZ**	447
O*	448	**PA**	449	**PB**	450
PC	451	**PD**	452	**PE**	453
PF	454	**PG**	455	**PH**	456
PI	457	**PJ**	458	**PK**	459
PL	460	**PM**	461	**PN**	462
PÑ	463	**PO**	464	**PP**	465
PQ	466	**PR**	467	**PS**	468
PT	469	**PU**	470	**PV**	471
PW	472	**PX**	473	**PY**	474
PZ	475	**P***	476	**QA**	477
QB	478	**QC**	479	**QD**	480
QE	481	**QF**	482	**QG**	483
QH	484	**QI**	485	**QJ**	486
QK	487	**QL**	488	**QM**	489
QN	490	**QÑ**	491	**QO**	492
QP	493	**QQ**	494	**QR**	495
QS	496	**QT**	497	**QU**	498
QV	499	**QW**	500	**QX**	501
QY	502	**QZ**	503	**Q***	504
RA	505	**RB**	506	**RC**	507
RD	508	**RE**	509	**RF**	510

Tabla

Bloque	Número
RG	511
RJ	514
RM	517
RO	520
RR	523
RU	526
RX	529
R*	532
SC	535
SF	538
SI	541
SL	544
SÑ	547
SQ	550
ST	553
SW	556
SZ	559
TB	562
TE	565
TH	568
TK	571
TN	574
TP	577
TS	580
TV	583
TY	586
UA	589
UD	592
UG	595
UJ	598
UM	601
UO	604
UR	607
UU	610

Bloque	Número
RH	512
RK	515
RN	518
RP	521
RS	524
RV	527
RY	530
SA	533
SD	536
SG	539
SJ	542
SM	545
SO	548
SR	551
SU	554
SX	557
S*	560
TC	563
TF	566
TI	569
TL	572
TÑ	575
TQ	578
TT	581
TW	584
TZ	587
UB	590
UE	593
UH	596
UK	599
UN	602
UP	605
US	608
UV	611

Bloque	Número
RI	513
RL	516
RÑ	519
RQ	522
RT	525
RW	528
RZ	531
SB	534
SE	537
SH	540
SK	543
SN	546
SP	549
SS	552
SV	555
SY	558
TA	561
TD	564
TG	567
TJ	570
TM	573
TO	576
TR	579
TU	582
TX	585
T*	588
UC	591
UF	594
UI	597
UL	600
UÑ	603
UQ	606
UT	609
UW	612

Tabla

Bloque	Número
UX	613
U*	616
VC	619
VF	622
VI	625
VL	628
VÑ	631
VQ	634
VT	637
VW	640
VZ	643
WB	646
WE	649
WH	652
WK	655
WN	658
WP	661
WS	664
WV	667
WY	670
XA	673
XD	676
XG	679
XJ	682
XM	685
XO	688
XR	691
XU	694
XX	697
X*	700
YC	703
YF	706
YI	709
YL	712

Bloque	Número
UY	614
VA	617
VD	620
VG	623
VJ	626
VM	629
VO	632
VR	635
VU	638
VX	641
V*	644
WC	647
WF	650
WI	653
WL	656
WÑ	659
WQ	662
WT	665
WW	668
WZ	671
XB	674
XE	677
XH	680
XK	683
XN	686
XP	689
XS	692
XV	695
XY	698
YA	701
YD	704
YG	707
YJ	710
YM	713

Bloque	Número
UZ	615
VB	618
VE	621
VH	624
VK	627
VN	630
VP	633
VS	636
VV	639
VY	642
WA	645
WD	648
WG	651
WJ	654
WM	657
WO	660
WR	663
WU	666
WX	669
W*	672
XC	675
XF	678
XI	681
XL	684
XÑ	687
XQ	690
XT	693
XW	696
XZ	699
YB	702
YE	705
YH	708
YK	711
YN	714

Tabla

Bloque	Número
YÑ	715
YQ	718
YT	721
YW	724
YZ	727
ZB	730
ZE	733
ZH	736
ZK	739
ZN	742
ZP	745
ZS	748
ZV	751
ZY	754
***A**	757
***D**	760
***G**	763
***J**	766
***M**	769
***O**	772
***R**	775
***U**	778
***X**	781
***	784

Bloque	Número
YO	716
YR	719
YU	722
YX	725
Y*	728
ZC	731
ZF	734
ZI	737
ZL	740
ZÑ	743
ZQ	746
ZT	749
ZW	752
ZZ	755
***B**	758
***E**	761
***H**	764
***K**	767
***N**	770
***P**	773
***S**	776
***V**	779
***Y**	782

Bloque	Número
YP	717
YS	720
YV	723
YY	726
ZA	729
ZD	732
ZG	735
ZJ	738
ZM	741
ZO	744
ZR	747
ZU	750
ZX	753
Z*	756
***C**	759
***F**	762
***I**	765
***L**	768
***Ñ**	771
***Q**	774
***T**	777
***W**	780
***Z**	783

Capítulo 3

CURVAS ELÍPTICAS

3.1. CURVAS ELÍPTICAS EN $\mathbb{R}$

Hasta aquí hemos descrito lo que es el método RSA. Como se puede ver, las matemáticas que se usan, si bien no son elementales, tampoco requieren más que de un curso de Teoría de Números. Se puede hacer una variante de este método usando matemáticas más profundas. Esto es lo que trataremos a continuación. Para empezar, necesitamos saber qué son las curvas elípticas.

DEFINICIÓN 3.1.1 Una *curva elíptica* sobre un campo $\mathbb{F}$ (sólo tomaremos campos no degenerados, esto es, campos que tienen al menos un elemento diferente de 0, o equivalentemente, campos en los que $0 \neq 1$) es una curva que está dada por una ecuación de la forma:

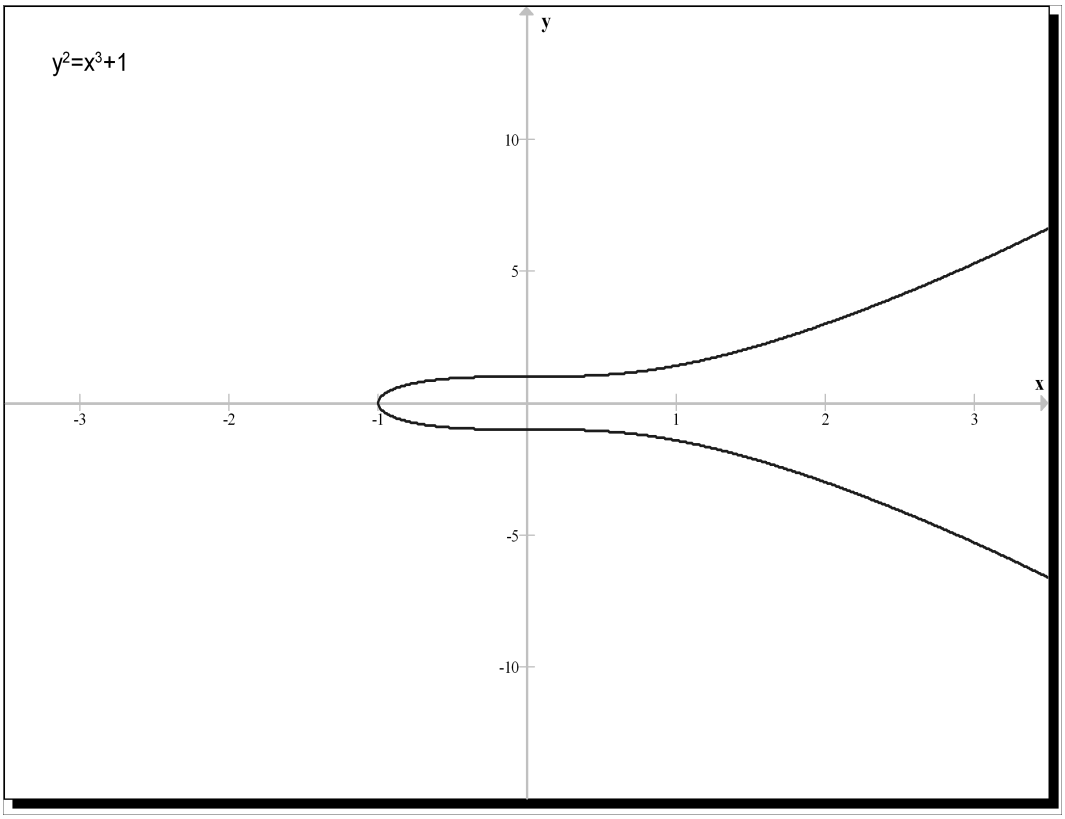
$$y^2 + axy + by = x^3 + cx^2 + dx + e, \text{ donde } a, b, c, d, e \in \mathbb{F},$$

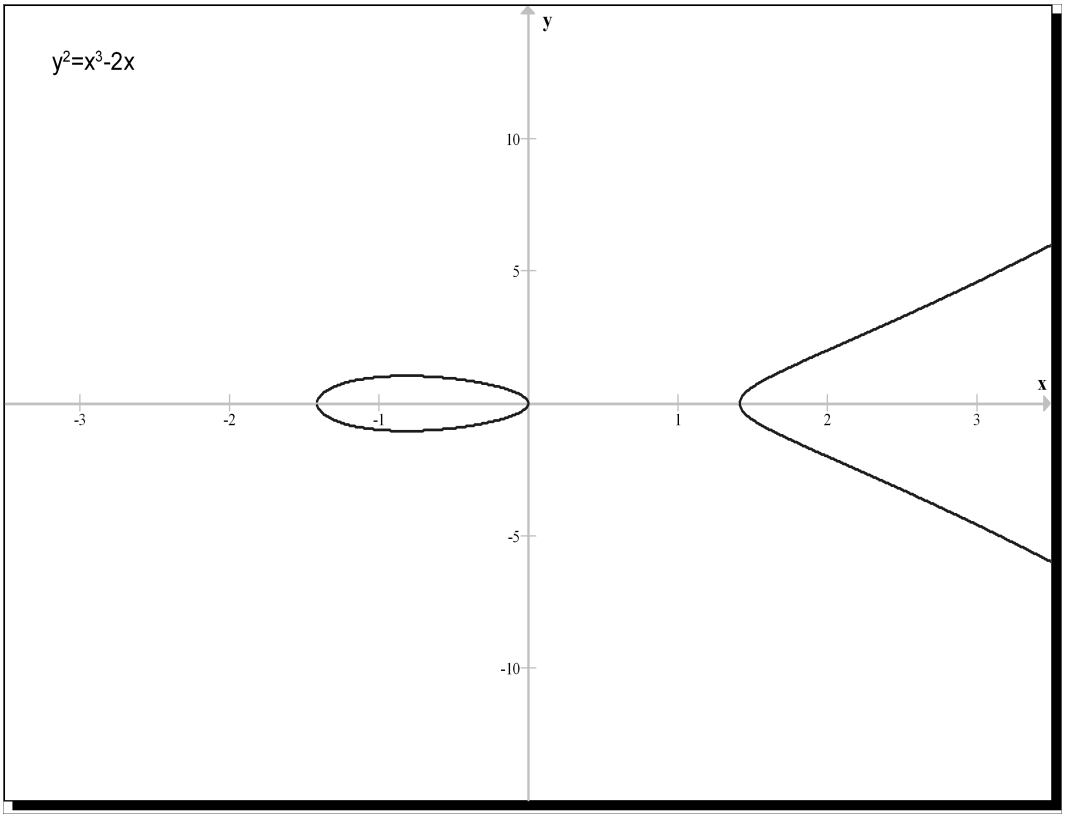
que además es una curva suave (esto quiere decir que las derivadas parciales $\frac{\partial f}{\partial x}$ y $\frac{\partial f}{\partial y}$ no se pueden anular ambas en un mismo elemento (x, y) de la curva (donde $f(x, y) = y^2 + axy + by - (x^3 + cx^2 + dx + e)$) o equivalentemente, que no existe una pareja (x, y) en la curva que sea solución común a las ecuaciónes $ay = 3x^2 + 2cx + d$ y $2y + ax + b = 0$).

Dada una curva elíptica fija, denotaremos por $S(\mathbb{F})$ al conjunto de soluciones de la ecuación añadiéndole el punto al infinito al cual denotaremos por ∞, es decir:

$$S(\mathbb{F}) = \{(x, y) \in \mathbb{F}^2 : y^2 + axy + by = x^3 + cx^2 + dx + e\} \cup \{\infty\}$$

Ejemplos de curvas elípticas





En el caso en que también estemos considerando un campo de extensión $\mathbb{K}$ de $\mathbb{F}$, también denotaremos:

$$S(\mathbb{K}) = \{(x, y) \in \mathbb{K}^2 : y^2 + axy + by = x^3 + cx^2 + dx + e\} \cup \{\infty\}.$$

Lo primero que haremos es mostrar que la ecuación de una curva elíptica puede ser escrita en forma más simple de acuerdo a la característica del campo sobre el cual estamos trabajando (recordemos que la característica de un campo $\mathbb{F}$ se define como el mínimo número natural p en $\mathbb{N}$ tal que para todo $a \neq 0$ en $\mathbb{F}$ se cumple que $\underbrace{p + p + \cdots + p}_{p-veces} = pa = 0$. En caso de no existir tal p como en el caso de $\mathbb{Z}$, se define la característica del campo como 0).

LEMA 3.1.2 La ecuación de una curva elíptica se puede simplificar, usando una transformación afín llegando a la forma:

(a) $y^2 = x^3 + cx^2 + dx + e$, si $\text{Car}(\mathbb{F}) = 3$.

(b) $y^2 = x^3 + dx + e$, si $\text{Car}(\mathbb{F}) \neq 2, 3$.

(c) $y^2 + axy = x^3 + cx^2 + e$, si $\text{Car}(\mathbb{F}) = 2$ y el coeficiente del término xy es diferente de cero.

(d) $y^2 + ay = x^3 + dx + e$, si $\text{Car}(\mathbb{F}) = 2$ y el coeficiente del término xy es cero.

DEMOSTRACIÓN.

(a) $\text{Car}(\mathbb{F}) = 3$.

En este caso, sabemos que $3z = 0$, o $z = -2z$, para toda $z \in \mathbb{F}$.

Proponemos el siguiente cambio de variable: $y = v + au + b$ y $x = u$. Sustituyendo en $y^2 + axy + by = x^3 + cx^2 + dx + e$, obtenemos

$$(v + au + b)^2 + au(v + au + b) + b(v + au + b) = u^3 + cu^2 + du + e,$$

de manera que:

$$v^2 + (au)^2 + b^2 + 2auv + 2abu + 2bv + auv + (au)^2 + abu + bv + abu + b^2 = u^3 + cu^2 + du + e.$$

Usando que $3z = 0$ para toda $z \in \mathbb{F}$, podemos simplificar, obteniendo:

$$v^2 + 2(au)^2 + 2b^2 + abu = u^3 + cu^2 + du + e.$$

Lo que se puede escribir como:

$$v^2 = u^3 + fu^2 + gu + h,$$

donde $f = c - 2a^2$, $g = d - ab$ y $h = e - 2b^2$. Ésta es la forma que buscábamos por lo que hemos terminado con el inciso (a).

(b) $\text{Car}(\mathbb{F}) \neq 2, 3$.

Aquí es conveniente recordar un par de cosas sobre la característica de un campo. Por definición, se dice que la característica de un campo $\mathbb{F}$ es el mínimo entero positivo k tal que $kz = 0$ para toda $z \in \mathbb{F}$, si existe tal entero k, si no existe, simplemente diremos que la característica de $\mathbb{F}$ es infinita. Lo primero que hay que mencionar es que si $kz = 0$ para algún entero positivo k y algún $z \in \mathbb{F} - \{0\}$, entonces $kw = 0$ para todos los elementos de $\mathbb{F}$. Esto se debe a que

$$\begin{aligned} kw &= \underbrace{w + \cdots + w}_{k \quad veces} = zz^{-1}w + \cdots + zz^{-1}w \\ &= (z + \cdots + z)z^{-1}w = 0 \cdot z^{-1}w = 0 \end{aligned}$$

Entonces, se puede definir la característica de $\mathbb{F}$ como el mínimo entero positivo k para el que existe un elemento $z \in \mathbb{F} - \{0\}$ tal que $kz = 0$, si existe tal k, o si no se sigue diciendo que la característica de $\mathbb{F}$ es infinita.

De manera que, como estamos suponiendo que $\text{Car}(\mathbb{F}) \neq 2, 3$, tenemos que los elementos $2 = 1+1$ y $3 = 1+1+1$ no son cero. De modo que tampoco pueden ser iguales a cero los elementos $6 = 3+3$, $12 = 6+6$ y $24 = 12 + 12$. Y entonces podemos hablar de los elementos $\frac{1}{2}$, $\frac{1}{3}$, $\frac{1}{6}$, $\frac{1}{12}$ y $\frac{1}{24}$. Además recordemos que el elemento $\frac{1}{2}z$ es la mitad de z en el sentido de que $\frac{1}{2}z + \frac{1}{2}z = 1 \cdot \frac{1}{2}z + 1 \cdot \frac{1}{2}z = (1+1)\frac{1}{2}z = 2(\frac{1}{2})z = 1 \cdot z = z$. Así que $\frac{1}{2}z + \frac{1}{2}z = z$. De la misma manera se muestra que $\frac{1}{3}z$ es la tercera parte de z, $\frac{1}{6}z$ es la sexta parte de z, etc.

Dicho todo esto, estamos listos para mostrar el inciso (b) de este lema. Para lo cual proponemos el siguiente cambio de variable:

$$\begin{gathered} y = v - \tfrac{1}{2}au + \tfrac{1}{6}ac + \tfrac{1}{24}a^3 - \tfrac{1}{2}b, \quad \text{y} \\ x = u - \tfrac{1}{3}c - \tfrac{1}{12}a^2. \end{gathered}$$

Al sustituirlo en $y^2 + axy + by = x^3 + cx^2 + dx + e$, obtenemos:

$$(v - \tfrac{1}{2}au + \tfrac{1}{6}ac + \tfrac{1}{24}a^3 - \tfrac{1}{2}b)^2 +$$
$$a(u - \tfrac{1}{3}c - \tfrac{1}{12}a^2)(v - \tfrac{1}{2}au + \tfrac{1}{6}ac + \tfrac{1}{24}a^3 - \tfrac{1}{2}b) +$$
$$b(v - \tfrac{1}{2}au + \tfrac{1}{6}ac + \tfrac{1}{24}a^3 - \tfrac{1}{2}b) =$$
$$(u - \tfrac{1}{3}c - \tfrac{1}{12}a^2)^3 + c(u - \tfrac{1}{3}c - \tfrac{1}{12}a^2)^2 + d(u - \tfrac{1}{3}c - \tfrac{1}{12}a^2) + e.$$

Simplemente desarrollando y pasando todo al primer lado, tenemos:

$$v^2 + \tfrac{1}{4}(au)^2 + (\tfrac{1}{6}ac + \tfrac{1}{24}a^3 - \tfrac{1}{2}b)^2 - auv - au(\tfrac{1}{6}ac + \tfrac{1}{24}a^3 - \tfrac{1}{2}b)$$
$$+2v(\tfrac{1}{6}ac + \tfrac{1}{24}a^3 - \tfrac{1}{2}b) + auv - \tfrac{1}{2}(au)^2 + a^2u\tfrac{1}{2}(\tfrac{1}{3}c + \tfrac{1}{12}a^2)$$
$$-\tfrac{1}{2}abu - a(\tfrac{1}{3}c + \tfrac{1}{12}a^2)(-\tfrac{1}{2}au + \tfrac{1}{6}ac + \tfrac{1}{24}a^3 - \tfrac{1}{2}b) +$$
$$-a(\tfrac{1}{3}c + \tfrac{1}{12}a^2)v + bv - \tfrac{1}{2}abu + b(\tfrac{1}{6}ac + \tfrac{1}{24}a^3 - \tfrac{1}{2}b)$$
$$-u^3 + 3(\tfrac{1}{3}c + \tfrac{1}{12}a^2)u^2 - 3(\tfrac{1}{3}c + \tfrac{1}{12}a^2)^2u + (\tfrac{1}{3}c + \tfrac{1}{12}a^2)^3 - cu^2$$
$$+2cu(\tfrac{1}{3}c + \tfrac{1}{12}a^2) - c(\tfrac{1}{3}c + \tfrac{1}{12}a^2)^2 - du + d(\tfrac{1}{3}c + \tfrac{1}{12}a^2) - e = 0.$$

Analicemos cuáles son los términos que tienen a u^2. En el renglón 1 aparece $\frac{1}{4}a^2$, en el 2, $-\frac{1}{2}a^2$, en el 5, $3(\frac{1}{3}c + \frac{1}{12}a^2)$ y $-c$. Por lo que a la hora de sumarlos desaparecen todos.

Los términos que acompañan a uv son, en el renglón 1, $-a$ y en el 2, a, por lo que también a éstos les podemos decir adios.

Ahora veamos quiénes acompañan a v. En el renglón 2 está $2(\frac{1}{6}ac + \frac{1}{24}a^3 - \frac{1}{2}b)$, en el 4, $-a(\frac{1}{3}c + \frac{1}{12}a^2)$ y también b. De modo que éstos también desaparecen.

Ahora quitamos todos los términos mencionados. Con esto, ya queda la ecuación como queríamos pues sólo apareceran los términos v^2 y aquéllos que tienen a u^3 y u (además del independiente). Ya nada más para no dejar, veremos cómo quedan al final. Lo primero que hacemos es simplemente borrar los términos anunciados arriba.

$$v^2 + (\tfrac{1}{6}ac + \tfrac{1}{24}a^3 - \tfrac{1}{2}b)^2 - au(\tfrac{1}{6}ac + \tfrac{1}{24}a^3 - \tfrac{1}{2}b) - \tfrac{1}{2}abu +$$
$$+a^2u\tfrac{1}{2}(\tfrac{1}{3}c + \tfrac{1}{12}a^2) - a(\tfrac{1}{3}c + \tfrac{1}{12}a^2)(-\tfrac{1}{2}au + \tfrac{1}{6}ac + \tfrac{1}{24}a^3 - \tfrac{1}{2}b) -$$
$$-\tfrac{1}{2}abu + b(\tfrac{1}{6}ac + \tfrac{1}{24}a^3 - \tfrac{1}{2}b) - u^3 - 3(\tfrac{1}{3}c + \tfrac{1}{12}a^2)^2u +$$
$$+(\tfrac{1}{3}c + \tfrac{1}{12}a^2)^3 + 2cu(\tfrac{1}{3}c + \tfrac{1}{12}a^2) - c(\tfrac{1}{3}c + \tfrac{1}{12}a^2)^2$$
$$-du + d(\tfrac{1}{3}c + \tfrac{1}{12}a^2) - e = 0.$$

Agrupamos los términos que contienen a u y los independientes, dejando a v^2 solo de un lado de la igualdad.

$$v^2 = u^3 + [a(\tfrac{1}{6}ac + \tfrac{1}{24}a^3 - \tfrac{1}{2}b) - a^2\tfrac{1}{2}(\tfrac{1}{3}c + \tfrac{1}{12}a^2) - \tfrac{1}{2}ab -$$
$$-\tfrac{1}{2}a^2(\tfrac{1}{3}c + \tfrac{1}{12}a^2) - \tfrac{1}{2}ab + 3(\tfrac{1}{3}c + \tfrac{1}{12}a^2)^2 - 2c(\tfrac{1}{3}c + \tfrac{1}{12}a^2) + d]u$$
$$+[-(\tfrac{1}{6}ac + \tfrac{1}{24}a^3 - \tfrac{1}{2}b)^2 + a(\tfrac{1}{3}c + \tfrac{1}{12}a^2)(\tfrac{1}{6}ac + \tfrac{1}{24}a^3 - \tfrac{1}{2}b) -$$
$$-b(\tfrac{1}{6}ac + \tfrac{1}{24}a^3 - \tfrac{1}{2}b) - (\tfrac{1}{3}c + \tfrac{1}{12}a^2)^3 + c(\tfrac{1}{3}c + \tfrac{1}{12}a^2)^2$$
$$-d(\tfrac{1}{3}c + \tfrac{1}{12}a^2) + e].$$

Ésta es la expresión final que buscábamos.

(c) $\mathrm{Car}(\mathbb{F}) = 2$ y el coeficiente del término xy (que se llama a) es diferente de cero.

En este caso hacemos el cambio de variable

$$y = v + m \quad \text{y} \quad x = u + ba^{-1},$$

(donde $m = a^{-1}((ba^{-1})^2 + d)$, y sustituimos en la ecuación $y^2 + axy + by = x^3 + cx^2 + dx + e$. Obtenemos:

$$(v+m)^2 + a(u + ba^{-1})(v+m) + b(v+m)$$
$$= (u + ba^{-1})^3 + c(u + ba^{-1})^2 + d(u + ba^{-1}) + e.$$

Como $\mathrm{Car}(\mathbb{F}) = 2$, $2z = 0$ y $3z = z$ para cada $z \in \mathbb{F}$. De manera que cuando desarrollamos esta ecuación, quitando todos los términos que tengan un 2 y sustituyendo $3z$ por z en donde aparece un 3, tenemos que:

$$v^2 + m^2 + auv + aum + bv + bm + bv + bm = u^3 +$$
$$u^2ba^{-1} + ub^2a^{-2} + b^3a^{-3} + cu^2 + cb^2a^{-2} + du + dba^{-1} + e.$$

Tenemos otros dos términos dobles, a saber, $2bv$ y $2bm$. Entonces los podemos quitar y sustituir el valor de m con lo que tendremos:

$$v^2 + a^{-2}((ba^{-1})^2 + d)^2 + auv + aua^{-1}((ba^{-1})^2 + d) = u^3 +$$
$$u^2ba^{-1} + ub^2a^{-2} + b^3a^{-3} + cu^2 + cb^2a^{-2} + du + dba^{-1} + e.$$

Si pasamos todos los términos que tienen a u al primer término de la igualdad y vemos quién lo acompaña veremos que se trata de $(ba^{-1})^2 + d - b^2a^{-2} - d$. Por lo que este término desaparece. Éste es el término que queríamos que desapareciera, por lo que ya prácticamente terminamos este inciso. Como antes, veamos un poco más cómo queda la ecuación.

$$v^2 + a^{-2}((ba^{-1})^2 + d)^2 + auv =$$
$$u^3 + u^2ba^{-1} + b^3a^{-3} + cu^2 + cb^2a^{-2} + dba^{-1} + e.$$

Acomodando queda así:

$$v^2 + auv =$$
$$u^3 + (ba^{-1} + c)u^2 - a^{-2}((ba^{-1})^2 + d)^2 + b^3a^{-3} + cb^2a^{-2} + dba^{-1} + e.$$

Que es lo que buscábamos.

(d) $\mathrm{Car}(\mathbb{F}) = 2$ y el coeficiente del término xy (que se llama a) es cero.

Para este caso hacemos $y = v$ y $x = u + c$. Y como siempre, los sustituimos en la ecuación $y^2 + axy + by = x^3 + cx^2 + dx + e$, obteniendo:

$$v^2 + bv = (u + c)^3 + c(u + c)^2 + d(u + c) + e.$$

Desarrollando tenemos que:

$$v^2 + bv = u^3 + 3u^2c + 3uc^2 + c^3 + cu^2 + 2uc^2 + c^3 + du + dc + e.$$

Como $\text{Car}(\mathbb{F}) = 2$, los números 3 desaparecen y el término $2uc^2$ se quita. Al hacer esto, obtenemos los sumandos u^2c y cu^2 que al sumarlos se cancelan, lo mismo ocurre con los términos c^3. Por tanto la ecuación se transforma en:

$$v^2 + bv = u^3 + (c^2 + d)u + dc + e.$$

Que ya está como queríamos.

■

Ahora nos concentraremos en el caso en que $\text{Car}(\mathbb{F}) \neq 2, 3$. Según el lema que probamos, usando una transformación afín podemos cambiar la curva original ($y^2 + axy + by = x^3 + cx^2 + dx + e$) por una curva de la forma $y^2 = x^3 + dx + e$. Con esto, podemos trabajar con estas nuevas expresiones que son más simples. El siguiente resultado nos dice un criterio para comprobar que una curva del nuevo tipo es elíptica.

LEMA 3.1.3 La curva que tiene por ecuación $y^2 = x^3 + dx + e$ es elíptica si y sólo si el polinomio $x^3 + dx + e$ no tiene raíces múltiples.

DEMOSTRACIÓN.

($\Rightarrow$) Supongamos que la curva es elíptica. De acuerdo con la definición, tenemos que las parciales $\frac{\partial f}{\partial x}$ y $\frac{\partial f}{\partial y}$ no se pueden anular en un mismo punto de la curva, donde $f(x, y) = y^2 - x^3 - dx - e$. Es decir, no existe ningún punto (x, y) de la curva tal que las siguientes ecuaciones se cumplen ambas para el punto (x, y):

$$2y = 0 \text{ y } 3x^2 + d = 0$$

Supongamos, para buscar una contradicción, que el polinomio $p(x) = x^3 + dx + e$ tiene alguna raíz múltiple, digamos que u es esta raíz. Por definición esto quiere decir que el polinomio $(x - u)^2$ divide a $p(x)$. De modo que $p(x) = (x - u)^2(x - a)$ para alguna $a \in \mathbb{F}$, en principio aquí tendríamos que poner $p(x) = (x - u)^2 g(x)$ para algún polinomio $g(x)$, pero si observamos la forma que tiene $p(x)$, a $g(x)$ no le queda más remedio que ser de la forma $x - a$. Entonces:

$$x^3 + dx + e = (x^2 - 2ux + u^2)(x - a) =$$
$$x^3 - (2u + a)x^2 + (2au + u^2)x - au^2.$$

Igualando los coeficientes tenemos que

$$2u + a = 0;\ 2au + u^2 = d \quad \text{y} \quad au^2 = -e.$$

Combinando las dos primeras igualdades tenemos que:

$$-4u^2 + u^2 = d$$

De donde tenemos que $3u^2 + d = 0$

Por tanto las parciales de f se anulan ambas en el punto $(u, 0)$. Esto es absurdo pues estamos suponiendo que la curva es elíptica.

Por tanto $p(x)$ no tiene raíces múltiples.

($\Leftarrow$) Ahora supongamos que el polinomio $p(x)$ no tiene raíces múltiples. También supongamos que la curva no es elíptica. Entonces existe un punto (u, v) de la curva en el que las dos derivadas parciales de f se anulan. Así que $v^2 = u^3 + du + e$, $2v = 0$ y $3u^2 + d = 0$. Como $\mathbb{F}$ no tiene característica 2, $v = 0$. Vamos a mostrar que u es una raíz múltiple de $p(x)$. Para esto, bastará mostrar que existe una $a \in \mathbb{F}$ tal que

$$\begin{aligned} x^3 + dx + e &= (x - u)^2(x - a) \\ &= (x^2 - 2ux + u^2)(x - a) \\ &= x^3 - (2u + a)x^2 + (2au + u^2)x - au^2. \end{aligned}$$

De modo que necesitamos encontrar una $a \in \mathbb{F}$ para la que se satisfagan las siguientes ecuaciones

$$2u + a = 0,\ 2au + u^2 = d \text{ y } -au^2 = e.$$

De la primera se ve cómo se tiene que proponer a a. Hacemos $a = -2u$. Automáticamente se satisface la primera ecuación. Sustituyendo esta a en la segunda ecuación, deberíamos tener que $-4u^2 + u^2 = d$. Esto también es cierto porque, como las parciales se anulaban en (u, v), habíamos obtenido que $3u^2 + d = 0$. Finalmente, ya habíamos obtenido que $v = 0$ y que $v^2 = u^3 + du + e$. De modo que $u^3 + du + e = 0$ y, como sabíamos que $d = -3u^2$, obtenemos que $-2u^3 + e = 0$. De donde $-au^2 = 2u^3 = e$. Hemos comprobado las tres ecuaciones que debe satisfacer a. Por tanto u es una raíz múltiple de $p(x)$. Esta contradicción completa la prueba de que la curva es elíptica y con esto terminamos la prueba del lema.

■

3.2. LAS CURVAS ELÍPTICAS COMO GRUPOS

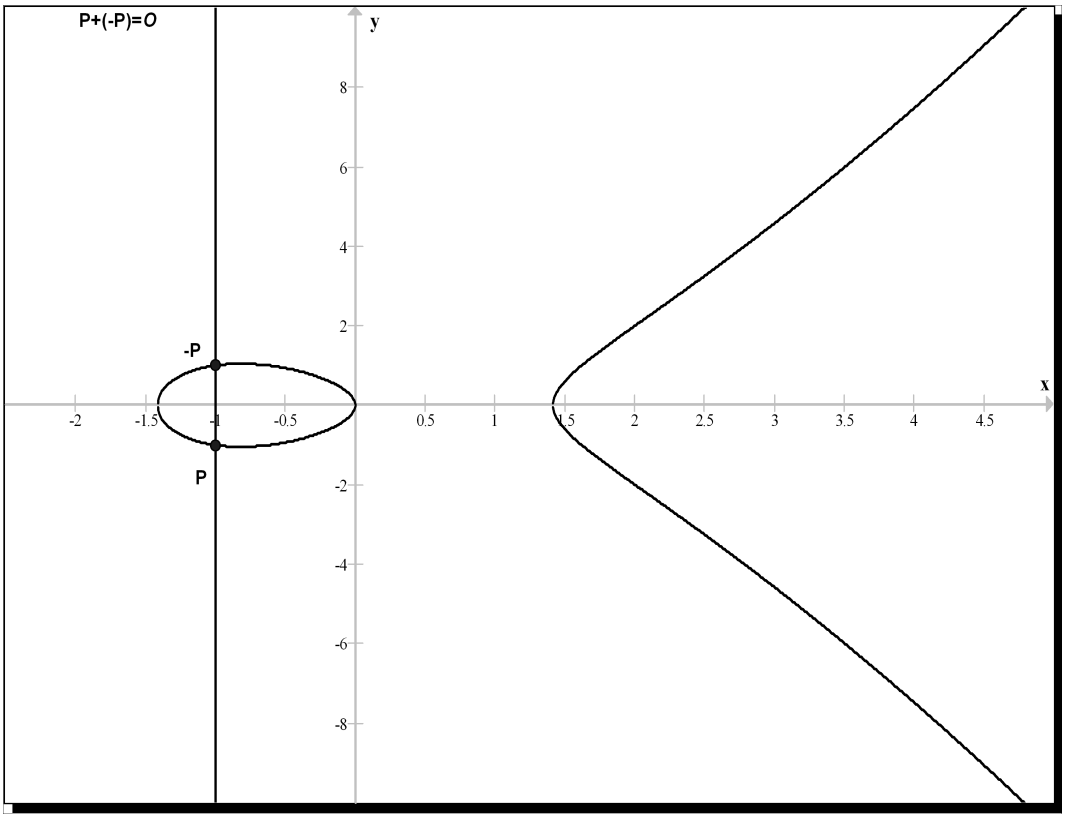
En esta sección trabajaremos con el campo de los números reales. De acuerdo con el Lema 3.1.2, podemos concentrarnos en una ecuación elíptica de la forma $y^2 = x^3 + dx + e$. En esta sección definiremos una operación en el conjunto de los puntos sobre la curva. Primero diremos cómo se define la operación, para esto nos guiamos con las gráficas y más tarde daremos las justificaciones necesarias. Definimos $S = \{(x, y) \in \mathbb{R}^2 : y^2 = x^3 + dx + e\} \cup \{\infty\}$.

Dados P, Q en S definimos $-P$ y $P + Q$ de acuerdo con las siguientes reglas.

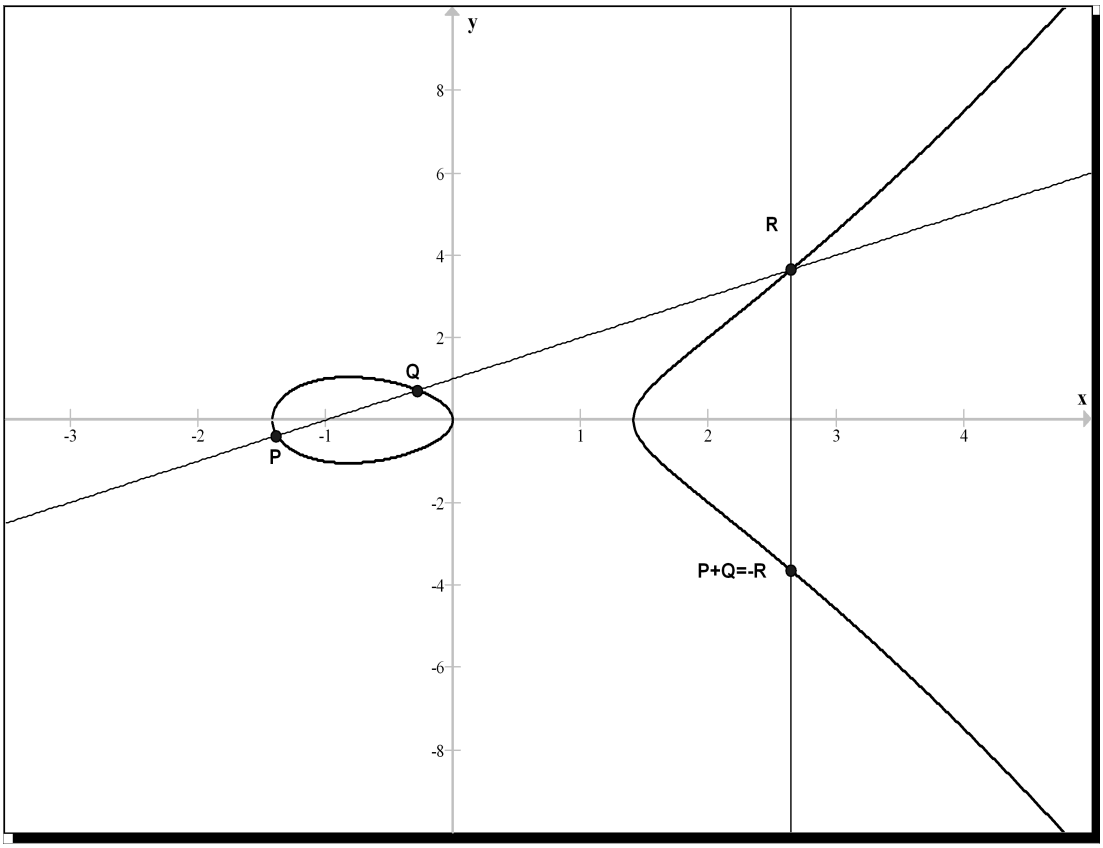
(1) Si P es el punto al infinito, definimos $-P = \infty$ y $\infty + Q = Q = Q + \infty$ para toda $Q \in S$. De esta manera, ∞ es el neutro aditivo de S.

(2) Si $P = (x, y) \in S - \{\infty\}$, notemos que $y^2 = x^3 + dx + e$, y entonces $(-y)^2 = x^3 + dx + e$, por lo que $(x, -y) \in P - \{\infty\}$. Por tanto podemos definir $-P = (x, -y)$ (¡ojo!, es importante no confundir $-P$ con $(-x, -y)$).

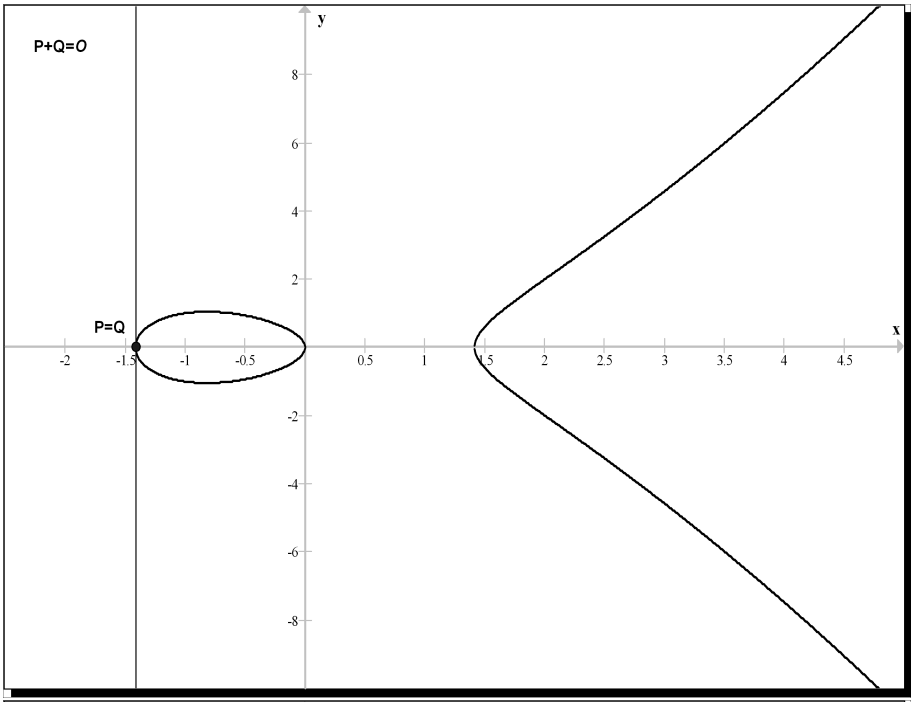
Para que nuestra definición sea congruente con lo que dijimos arriba, definimos $P + (-P) = \infty = (-P) + P$.

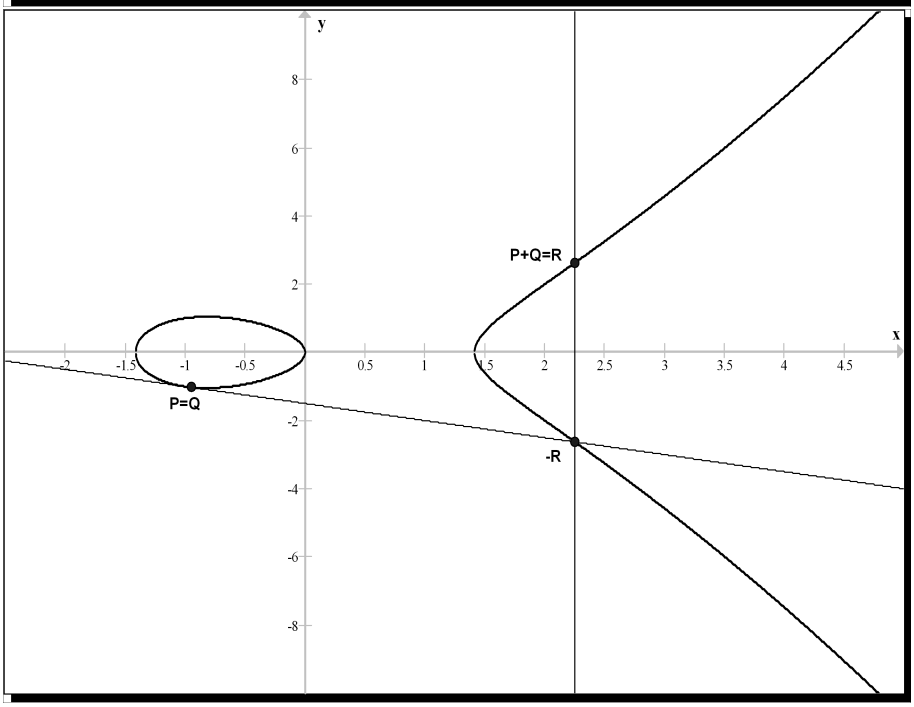


(3) Si P y Q tienen diferente coordenada x, entonces la línea que une a P con Q intersecta a la curva en exactamente otro punto R, a menos que esta recta sea tangente en P o en Q. En el primer caso, definimos $P + Q = -R = Q + P$ ($-R$ como se definió en (2)), en el segundo $P + Q = P$ y en el tercero $P + Q = Q$.



(4) Si $P = Q$, sea l la recta tangente a la curva en el punto P. Entonces l intersecta a la curva en otro punto (único) R o l ya no vuelve a intersectar a la curva (cuando l es vertical). En el primer caso definimos $P + Q = -R$, en el segundo, $P + Q = \infty$.


P+Q=O
P=Q
y
x
8
6
4
2
-2
-4
-6
-8
-2
-1.5
-1
-0.5
0.5
1
1.5
2
2.5
3
3.5
4
4.5


y
x
P+Q=R
P=Q
-R
8
6
4
2
-2
-4
-6
-8
-2
-1.5
-1
-0.5
0.5
1
1.5
2
2.5
3
3.5
4
4.5

Ahora vamos a mostrar que todas las definiciones son justificadas. Haremos el álgebra necesaria para comprobar las afirmaciones que hicimos sobre las intersecciones de las rectas con la curva.

Primero veremos que si $P \neq \pm Q$ y P, Q pertenecen a la curva (llamémosle $\mathcal{C}$ a la curva), entonces la recta que pasa por P y por Q (llamémosle $\mathcal{L}$) intersecta a la curva en exactamente otro punto.

Para esto ponemos $P = (x_1, y_1)$, $Q = (x_2, y_2)$ y sea $y = \alpha x + \beta$ la ecuación de la recta ($\mathcal{L}$) que pasa por ellos. La podemos poner así porque al ser $P \neq -Q$, entonces la recta no es vertical. Además $\alpha = \frac{y_2 - y_1}{x_2 - x_1}$ y $\beta = y_1 - \alpha x_1$.

En general un punto (x, y) pertenece a $\mathcal{L} \cap \mathcal{C}$ si:

$$y = \alpha x + \beta \text{ (por estar en } \mathcal{L}\text{), y}$$
$$y^2 = x^3 + dx + e \text{ (por estar en } \mathcal{C}\text{).}$$

De manera que

$$(\alpha x + \beta)^2 = x^3 + dx + e.$$

De modo que el número x debe ser raíz del polinomio

$$q(x) = x^3 - (\alpha x + \beta)^2 + dx + e, \text{ que es igual a}$$
$$q(x) = x^3 - \alpha^2 x^2 + (d - 2\alpha\beta)x + e - \beta^2.$$

Sabemos que un polinomio de grado 3 puede tener a lo más 3 raíces. El polinomio $q(x)$ ya tiene dos (x_1 y x_2) así que ya sólo podría tener una raíz más y, como el número y está completamente determinado por el número x (cuando $(x, y) \in \mathcal{L}$), entonces a lo más podemos tener un tercer punto en $\mathcal{L} \cap \mathcal{C}$.

Ahora veamos que, efectivamente, hay un tercer punto. Una tercera raíz x_3 del polinomio $q(x)$ deberá satisfacer que:

$$q(x) = (x - x_1)(x - x_2)(x - x_3) =$$
$$x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3.$$

Igualando el coeficiente de x^2, se debe tener que:

$$\alpha^2 = x_1 + x_2 + x_3.$$

Esto ya nos da oportunidad de conocer x_3 en términos de x_1 y x_2, y la ecuación de la recta nos permite conocer a y_3. Sustituyendo, tenemos:

$$x_3 = (\tfrac{y_2-y_1}{x_2-x_1})^2 - x_1 - x_2, \text{ y}$$
$$y_3 = \alpha x_3 + \beta = (\tfrac{y_2-y_1}{x_2-x_1})x_3 + y_1 - (\tfrac{y_2-y_1}{x_2-x_1})x_1 = (\tfrac{y_2-y_1}{x_2-x_1})(x_3 - x_1) + y_1.$$

Teniendo los valores para x_3 y y_3 nos falta verificar que el punto (x_3, y_3) efectivamente está en la recta y en la curva. Con la recta no hay problema pues el y_3 se despejó de su ecuación. Podríamos hacer las cuentas necesarias para ver que el punto (x_3, y_3) satisface la ecuación de la curva, pero eso se ve muy complicado, en cambio, haremos un truco de polinomios, a ver que le parece.

Para encontrar x_3 supusimos que existía, factorizamos a $q(x)$ y vimos qué condiciones tenía que cumplir x_3. Veamos que no necesitamos suponer que existe x_3 sino que podemos comprobar su existencia.

Sabemos que x_1 y x_2 sí son raíces de $q(x)$ y son diferentes. De manera que el polinomio $(x-x_1)(x-x_2)$ divide a $q(x)$. Por tanto existe un polinomio $g(x)$ tal que

$$q(x) = (x - x_1)(x - x_2)g(x).$$

Como $q(x)$ es de grado 3, a $g(x)$ no le queda más que ser de grado 1. Además el coeficiente de x^3 en $q(x)$ es 1, entonces el polinomio de x en $g(x)$ es también 1. Por tanto, $g(x) = x - x_3$ para alguna $x_3 \in \mathbb{R}$ (¡ojo! justo aquí estamos mostrando que existe x_3). Así pues,

$$q(x) = (x - x_1)(x - x_2)(x - x_3).$$

A partir de aquí, ya pudimos despejar x_3 de la ecuación $\alpha^2 = x_1 + x_2 + x_3$ y pudimos definir $y_3 = \alpha x_3 + \beta$.

Como x_3 es raíz de $q(x)$, por la definición de $q(x)$, tenemos que

$$(\alpha x_3 + \beta)^2 = x_3^3 + dx_3 + e.$$

. Por tanto $y_3^2 = x_3^3 + dx_3 + e$, que es lo que queríamos verificar.

Ahora analicemos qué ocurre cuando $P = Q = (x_1, y_1)$. Consideremos la recta tangente a la curva, que pasa por P. Ponemos la ecuación de la recta en la forma $y = \alpha x + \beta$ (el caso en que la recta es vertical hay que hacerlo aparte, ya no lo haremos para no hacer esto tan largo). Si tomamos puntos sobre la curva, cada uno de ellos debe satisfacer la ecuación $y^2 = x^3 + dx + e$ como antes, si un punto está tanto en la recta que tiene por ecuación $y = \alpha x + \beta$ como en la curva $y^2 = x^3 + dx + e$, este punto deberá satisfacer la ecuación $(\alpha x + \beta)^2 = x^3 + dx + e$ por lo que este punto es raíz del polinomio $q(x) = x^3 - (\alpha x + \beta)^2 + dx + e$. Podemos pensar que y está en función de x (al menos localmente) y poner

$$(y(x))^2 = x^3 + dx + e.$$

Esto nos permite derivar para obtener:

$$2y(x)y'(x) = 3x^2 + d.$$

De modo que

$$\frac{dy}{dx} = \frac{3x^2+d}{2y}.$$

Como la recta debe ser tangente a la curva en el punto debemos tener que:

$$\alpha = \frac{3x_1^2+d}{2y_1}.$$

Ya que $P = Q$, x_1 debe ser una raíz doble del polinomio que se obtiene de sustituir la variable y de la ecuación de la recta en la variable y de la ecuación de la curva, es decir de:

$$q(x) = x^3 - (\alpha x + \beta)^2 + dx + e$$

Aquí podemos justificar la existencia de una segunda raíz x_3 del polinomio $q(x)$ en la misma manera que procedimos antes y obtener que tal raíz debe cumplir:

$$x_3 = \alpha^2 - x_1 - x_2 = \alpha^2 - 2x_1.$$

Y entonces podemos buscar y_3 tal que (x_3, y_3) esté en la recta $y = \alpha x_1 + \beta$ por lo que

$$y_3 = \alpha x_3 + \beta.$$

Pero $\beta = y - \alpha x$ y (x_1, y_1) está en la recta, entonces $\beta = y_1 - \alpha x_1$, por lo que

$$y_3 = \alpha x_3 + y_1 - \alpha x_1 = y_1 - \alpha(x_1 - x_3)$$

por lo que tenemos que

$$\begin{aligned} x_3 &= \alpha^2 - 2x_1 \\ \text{y} \quad y_3 &= y_1 - \alpha(x_1 - x_3) \end{aligned}$$

De donde, sustituyendo el valor de α obtenido arriba llegamos a que:

$$\begin{aligned} x_3 &= \Big(\frac{3x_1^2 + d}{2y_1}\Big)^2 - 2x_1 \\ \text{y} \quad y_3 &= y_1 - \Big(\frac{3x_1^2 + d}{2y_1}\Big)(x_1 - x_3) \end{aligned}$$

De acuerdo a lo anterior hemos demostrado que dados dos puntos en la curva elíptica, podemos trazar la recta que pasa por estos dos puntos, y en ella encontrar un tercer punto que esté tanto en la recta como en la curva. Este tercer punto estará definido a partir de los otros dos por las siguientes ecuaciones

1. Si $P = Q$ con $P = (x_1, y_1)$

$$\begin{aligned} x_3 &= \Big(\frac{3x_1^2 + d}{2y_1}\Big)^2 - 2x_1 \\ y_3 &= y_1 - (x_1 - x_3)\Big(\frac{3x_1^2 + d}{2y_1}\Big) \end{aligned}$$

2. Si $P \neq Q$ con $P = (x_1, y_1)$ y $Q = (x_2, y_2)$

$$\begin{aligned} x_3 &= \Big(\frac{y_2 - y_1}{x_2 - x_1}\Big)^2 - x_1 - x_2 \\ y_3 &= \Big(\frac{y_2 - y_1}{x_2 - x_1}\Big)(x_3 - x_1) + y_1 \end{aligned}$$

De acuerdo a la notación dada en las propiedades 3) y 4), las ecuaciones que encontramos corresponden al punto que denotamos por R, el cual es distinto de la suma de P y Q, por que recordemos que tanto en la propiedad 3) y 4) el punto asociado a $P+Q$ corresponde a $-R$. Como R tiene coordenadas (x_3, y_3) entonces $-R$ tendrá coordenadas $(x_3, -y_3)$. Debido a que posteriormente necesitaremos calcular en varias ocasiones la suma de dos puntos en la curva será importante escribir las ecuaciones de este tercer punto, lo cual se hará en el siguiente lema.

LEMA 3.2.1 Dados los puntos $P = (x_1, y_1)$ y $Q = (x_2, y_2)$ el punto asociado con $P + Q$ es el punto (x_3, y_3) en donde x_3 y y_3 están dados por:

1) Si $P = Q$ entonces

$$\begin{aligned} x_3 &= \Big(\frac{3x_1^2 + d}{2y_1}\Big)^2 - 2x_1 \\ y_3 &= -y_1 + (x_1 - x_3)\Big(\frac{3x_1^2 + d}{2y_1}\Big) \end{aligned}$$

2) Si $P \neq Q$ entonces

$$\begin{aligned} x_3 &= \Big(\frac{y_2 - y_1}{x_2 - x_1}\Big)^2 - x_1 - x_2 \\ y_3 &= \Big(\frac{y_2 - y_1}{x_2 - x_1}\Big)(x_1 - x_3) - y_1 \end{aligned}$$

Con esto terminamos de demostrar que la suma en S está bien definida. Ahora lo más interesante del asunto es comprobar que S es un grupo abeliano. Desafortunadamente la prueba completa de la asociatividad de la función está fuera del alcance de este trabajo. En principio, podríamos usar la fuerza bruta para hacer esto. Ya tenemos la definición y hasta tenemos fórmulas para calcular el resultado de la suma, sin embargo nada más de verlas se desanima cualquiera. Un mejor camino (el que vamos a seguir) consiste en suponer el siguiente resultado sobre rectas y usarlo para posteriormente demostrar que S es un grupo abeliano.

TEOREMA 3.2.2 Sean l_1, l_2 y l_3 tres rectas que intersectan a una cúbica en nueve puntos $P_1, P_2, ..., P_9$ (del plano proyectivo y contando

multiplicidad) y sean l'_1, l'_2 y l'_3 tres líneas que intersectan a la cúbica en nueve puntos $Q_1, Q_2, ..., Q_9$. Si $Q_i = P_i$ para toda $i \in \{1, 2, ..., 8\}$, entonces $Q_9 = P_9$.

TEOREMA 3.2.3 Dada una curva elíptica S (en los reales), el conjunto S con la operación que definimos arriba es un grupo abeliano.

DEMOSTRACIÓN.

Con lo que justificamos en los párrafos anteriores tenemos que la operación es cerrada, aunque tal vez valga la pena comentar el caso que se presenta en (3). En ese caso P y Q tienen diferente coordenada en x y se toma la recta l que pasa por ellos. En el caso en que l es tangente a la curva en P, se define $P + Q = P$ y en el caso en que l es tangente a la curva en Q, se define $P + Q = Q$. Notemos que no es posible que l sea tangente tanto en P como en Q pues esto implicaría que el polinomio que hemos usado ($q(x)$) tendría dos raíces dobles, una en la coordenada x de P y otra en la de Q, lo cual es imposible porque $q(x)$ es de grado 3. Con esto cerramos la discusión de que la suma está bien definida.

Si usted observa los 4 pasos de la definición de la suma, verá que se define de manera que es simétrica para P y Q. Por tanto, la suma es conmutativa. Definimos a ∞ como el neutro aditivo y, en todos los casos definimos ya al inverso aditivo.

Sólo nos falta ver la asociatividad. Para ver esto, tomemos tres puntos P, Q y R en S. Si alguno de los elementos P, Q o R es igual a ∞, supongamos para ilustrar que $P = \infty$, entonces, como ∞ es el neutro aditivo, $\infty + (Q + R) = Q + R = (\infty + Q) + R$. Por tanto, podemos suponer que ninguno es igual a ∞.

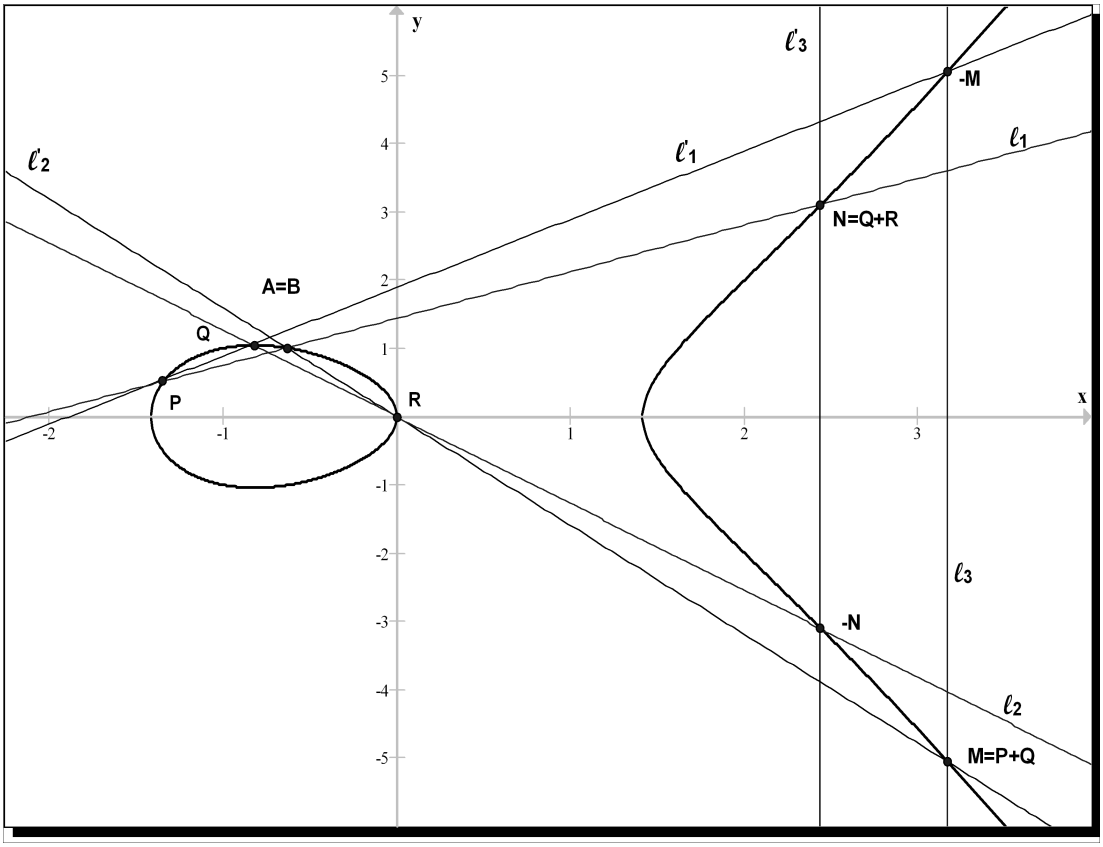
Ahora vamos a analizar el caso en que $Q + R = \infty$ (y $Q \neq \infty$ y $R \neq \infty$). En este caso, $Q = -R$. Si $Q = (u, v)$, entonces $R = (u, -v)$. Como $P+(Q+R) = P+\infty = P$, tenemos que mostrar que $(P+Q)+(-Q) = P$. Si $P = -Q$, entonces $(P+Q)+(-Q) = \infty+(-Q) = -Q = P$ y ya terminamos. Supongamos entonces que $P \neq -Q$. Sea $N = P + Q$. Entonces $N \neq \infty$. Sea l la recta que pasa por P y Q (en el caso en que $P = Q$, l es la recta tangente a la curva que pasa por P). De manera que, por definición, si K

es la otra intersección de l con la curva, entonces $N = -K$. Consideremos la recta $-l = \{(x, -y) \in \mathbb{R}^2 : (x, y) \in l\}$. Como P, Q y K pertenecen a l, $-P$, $-Q$ y $-K = N$ pertenecen a $-l$. Como l no es vertical, $-l$ tampoco es vertical. De modo que, si queremos calcular $N + (-Q)$, tenemos que ver cual es el otro punto en el que $-l$ intersecta a la curva. Este punto es precisamente $-P$, de modo que $N + (-Q) = -(-P) = P$ que es lo que queríamos probar.

Ahora podemos suponer que $Q+R \neq \infty$. Como la suma es conmutativa, también podemos suponer $P+Q \neq \infty$. De manera que estamos suponiendo que todos los puntos P, Q, R, $P+Q$ y $Q+R$ son diferentes de ∞ (y entonces todos ellos pertenecen a $\mathbb{R}^2$). Sean $M = P + Q$ y $N = Q + R$.

Consideremos las rectas:
(a) l_1 la que pasa por P, N, y sea A su tercer punto en S,
(b) l_2 la que pasa por Q y R, ésta pasa por $-N$, por definición,
(c) l_3 la que pasa por M y $-M$, ésta pasa por ∞, por definición,
(d) l_1' la que pasa por P y Q, ésta pasa por $-M$, por definición,
(e) l_2' la que pasa por M y R, y sea B su tercer punto en S,
(f) l_3' la que pasa por N y $-N$, ésta también pasa por ∞, por definición.

Entonces las rectas l_1, l_2 y l_3 en conjunto tienen a los puntos de la curva: P, N, $A = -(P + N)$, Q, R, M, $-N$, $-M$ e ∞. ¡Ojo!, aquí es importante notar que ∞ se puede pensar como el punto al infinito en el plano complejo que corresponde a las líneas verticales, pues ésa es la única interpretación que le dimos a ∞ en (c) y (f) al definir l_3 y l_3'. Por otra parte, las rectas l_1', l_2' y l_3' en conjunto tienen a los puntos de la curva: P, N, $B = -(M + R)$, Q, R, M, $-N$, $-M$ e ∞. De manera que las dos ternas de rectas tienen ocho puntos en común, que también pertenecen a la curva. Por tanto, el teorema 3.2.2 asegura que el noveno punto tiene que ser el mismo. Es decir, $A = B$. De donde, $-(P + N) = -(M + R)$. Por tanto, $P + (Q + R) = (P + Q) + R$. Hemos demostrado que la suma es asociativa y por tanto, la curva elíptica es un grupo abeliano. ■



EJEMPLO.

Consideremos la curva $y^2+y=x^3-x^2$. Esta curva no está puesta en la forma simplificada que hemos trabajado por lo que no hemos descrito todavía una manera de hacer, de su conjunto de puntos, un grupo. Sin embargo, usando las transformaciones lineales que propusimos antes, la simplificaremos y la convertiremos en grupo. En este ejemplo, calcularemos $2P=P+P$ y $3P=2P+P$, en donde $P=(0,0)$, observe que este punto está en la curva.

El cambio lineal que lleva esta curva a la forma simplificada es:

$$y=v-\tfrac{1}{2} \text{ y } x=u+\tfrac{1}{3}.$$

Sustituyendo en la ecuación original tenemos:

$$(v-\tfrac{1}{2})^2+(v-\tfrac{1}{2})=(u+\tfrac{1}{3})^3-(u+\tfrac{1}{3})^2, \quad \text{o}$$

$$v^2-v+\tfrac{1}{4}+v-\tfrac{1}{2}=u^3+u^2+\tfrac{1}{3}u+\tfrac{1}{27}-u^2-\tfrac{2}{3}u-\tfrac{1}{9}.$$

Simplificando se obtiene:

$$v^2 - \tfrac{1}{4} = u^3 - \tfrac{1}{3}u - \tfrac{2}{27}, \text{ o}$$

$$v^2 = u^3 - \tfrac{1}{3}u + \tfrac{19}{108}$$

Si aplicamos la misma transformación a P, obtenemos el punto Q dado por:

$$Q = (x - \tfrac{1}{3}, y + \tfrac{1}{2}) = (0 - \tfrac{1}{3}, 0 + \tfrac{1}{2}) = (-\tfrac{1}{3}, \tfrac{1}{2})$$

Ahora podemos calcular $2Q$ y $3Q$, recordemos las fórmulas que deducimos para $2Q$:

$$\begin{aligned} x_3 &= \Big(\frac{3x_1^2 + d}{2y_1}\Big)^2 - 2x_1, \quad \text{y} \\ y_3 &= -y_1 + (x_1 - x_3)\Big(\frac{3x_1^2 + d}{2y_1}\Big). \end{aligned}$$

De modo que:

$$\begin{aligned} x_3 &= \left(\frac{3(-1/3)^2 - (1/3)}{2(1/2)}\right)^2 - 2(-1/3) = \Big(\frac{0}{1}\Big)^2 + \frac{2}{3} = \frac{2}{3} \\ y_3 &= -\frac{1}{2} + \left(-\frac{1}{3} - \frac{2}{3}\right)\left(\frac{3(-1/3)^2 - 1/3}{2(1/2)}\right) = -\frac{1}{2} - 1(0) = -\frac{1}{2}. \end{aligned}$$

Por tanto

$$2Q = (\tfrac{2}{3}, -\tfrac{1}{2})$$

Una vez que hemos calculado $2Q$ podemos calcular $3Q$ con las ecuaciones

$$\begin{aligned} x_3 &= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \\ y_3 &= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1 \end{aligned}$$

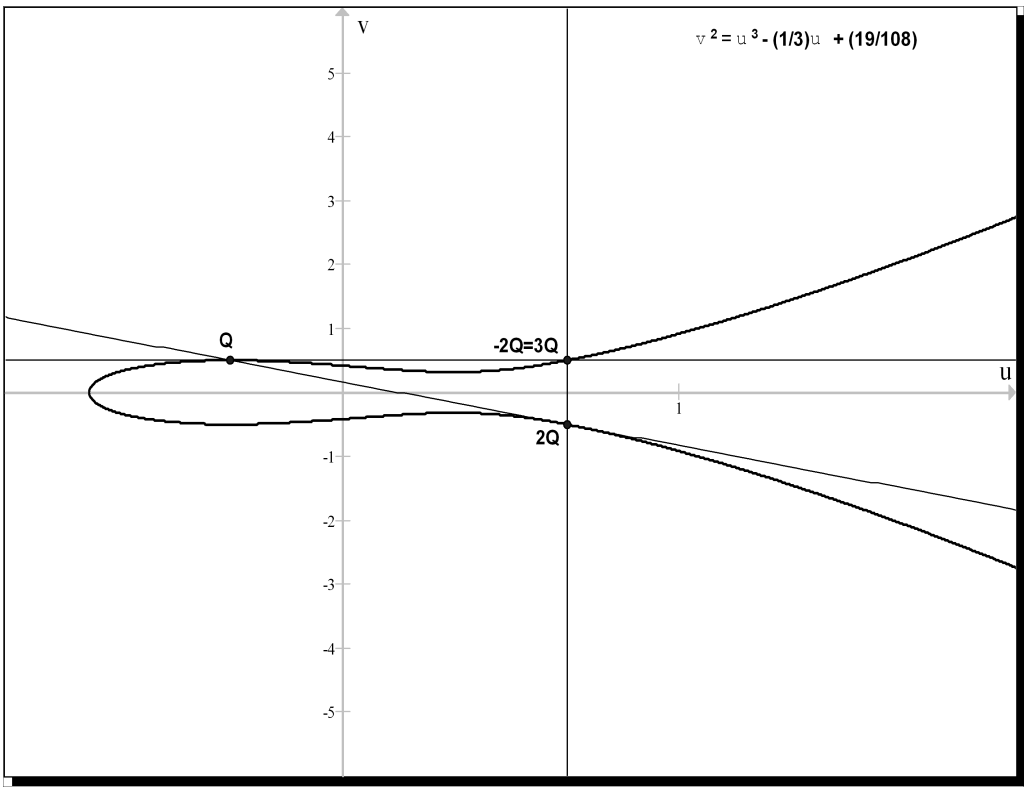
ya que $3Q = Q + 2Q$, por lo que podemos hacer

$$\begin{aligned} Q = (x_1, y_1) &= (-\tfrac{1}{3}, \tfrac{1}{2}) \quad \text{y} \\ 2Q = (x_2, y_2) &= (\tfrac{2}{3}, -\tfrac{1}{2}) \end{aligned}$$

de tal manera que

$$\begin{aligned} x_3 &= \Big(\frac{-\frac{1}{2}-\frac{1}{2}}{\frac{2}{3}+\frac{1}{3}}\Big)^2 + \frac{1}{3} - \frac{2}{3} = \big(\frac{-1}{1}\big)^2 - \frac{1}{3} = \frac{2}{3} \\ y_3 &= \Big(\frac{-\frac{1}{2}-\frac{1}{2}}{\frac{2}{3}+\frac{1}{3}}\Big)\Big(-\frac{1}{3}-\frac{2}{3}\Big) - \frac{1}{2} = \Big(\frac{-1}{1}\Big)(-1) - \frac{1}{2} = \frac{1}{2} \end{aligned}$$

por lo que $3Q = (\frac{2}{3}, \frac{1}{2})$. Como podemos notar los puntos $3Q$ y $2Q$ tienen la misma coordenada en x, y coordenada en y de mismo valor absoluto pero de signo contrario, lo cual quiere decir que $-3Q = 2Q$, es decir, $5Q = 0$. La gráfica de la ecuación simplificada así como los puntos correspondientes a Q, $2Q$ y $3Q$ se muestran en la siguiente gráfica, la cual tiene líneas de apoyo para poder localizar los puntos $2Q$ y $3Q$ gráficamente.



Como podemos notar entonces la línea que pasa por Q y $2Q$ es tangente a la curva en $2Q$. Esta recta no intersecta a la curva en ningún otro punto distinto a los mencionados, pero de acuerdo a las propiedades 3) y 4) debe

haber un tercer punto que este tanto en la recta como en la curva. Este tercer punto es $2Q$, debido a la propiedad 4), por esto la suma de Q y $2Q$ es $-2Q$.

Ahora bien, nuestro problema original era calcular $2P$ y $3P$, y no $2Q$ y $3Q$. Sin embargo podemos aplicar la transformación $y = v + 1/2$ y $x = u + 1/3$ a los puntos $2Q$ y $3Q$ y así obtendremos los puntos $2P$ y $3P$. Para el primero tendremos que como $2Q = (u, v) = (2/3, -1/2)$ entonces

$$\begin{aligned} y &= v + 1/2 = -1/2 + 1/2 = 0 \text{ y} \\ x &= u + 1/3 = 2/3 + 1/3 = 1 \end{aligned}$$

por lo que $2P = (0, 1)$. en el otro caso como $3Q = (u, v) = (2/3, 1/2)$ tendremos que

$$\begin{aligned} y &= v + 1/2 = +1/2 + 1/2 = 1 \text{ y} \\ x &= u + 1/3 = 2/3 + 1/3 = 1 \end{aligned}$$

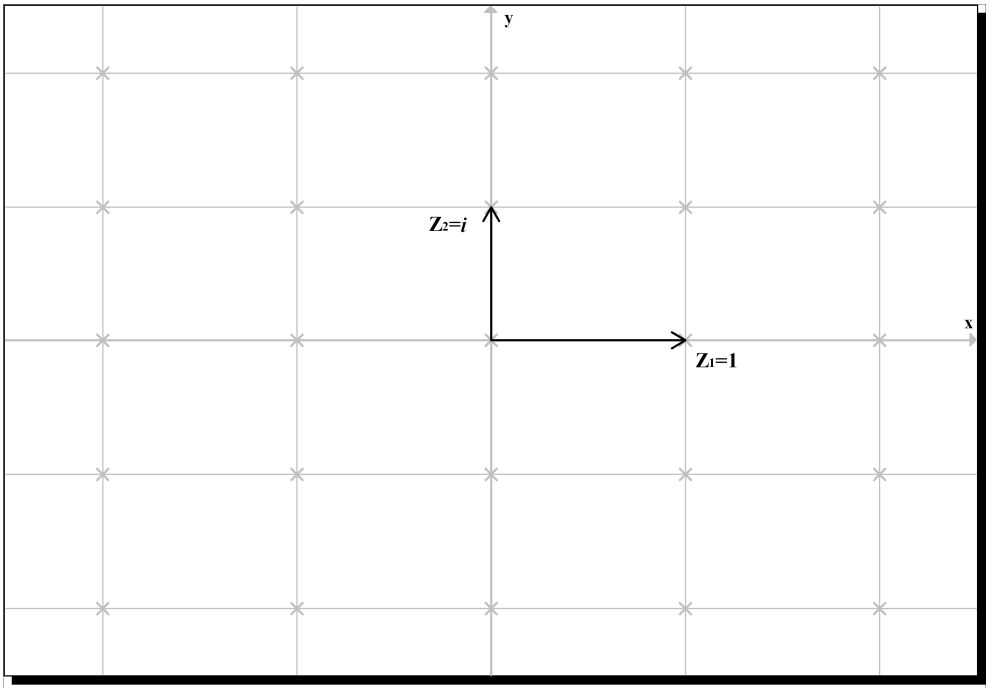
así, $3P = (1, 1)$, con lo cual concluimos nuestro ejemplo.

3.3. CURVAS ELÍPTICAS SOBRE LOS COMPLEJOS

Como hemos dicho antes, las curvas elípticas se pueden definir sobre cualquier campo. En los campos que no son de característica 2 ó 3, las curvas tienen una expresión muy simple ($y^2 = x^3 + dx + e$) y sus puntos, junto con el punto al infinito, constituyen un grupo. En particular, no hay ningún problema para considerarlas definidas para el campo de los números complejos. Las curvas para este caso no son tan usadas en criptografía pues se prefiere usar las curvas sobre campos finitos, como explicamos en la sección anterior. Sin embargo, estas curvas en los complejos tienen algunas propiedades matemáticas muy agradables que explicaremos en esta sección.

Estas propiedades son muy fáciles de enlistar pero dificiles de demostrar. Debido a esto, las personas que solamente estén interesadas en la parte de la criptografía en curvas elípticas pueden saltarse esta sección, ya que lo que concierne a la parte compleja no se usará para la criptografía.

Para enlistar las propiedades, necesitamos la definición de *latiz*, que no es más que un conjunto en el plano complejo de la forma $\{nz_1+mz_2 \in \mathbb{C} : n, m \in \mathbb{Z}\}$, donde z_1, z_2 son dos números complejos linealmente independientes (como elementos del espacio vectorial $\mathbb{R}^2$). En forma abreviada, podemos denotar esta latiz como $z_1\mathbb{Z}+z_2\mathbb{Z}$. Notemos que las latices son subgrupos de $\mathbb{C}$ y que si z_1, z_2 es la base canónica que consta de los números complejos 1 e i, entonces obtenemos la latiz que consta de todos los puntos de $\mathbb{R}^2$ que tienen ambas coordenadas enteras, a los elementos de esta latiz se les llama *enteros gaussianos*.



Ahora ya podemos adelantar lo que haremos con las curvas elípticas sobre $\mathbb{C}$. Empezaremos tomando una latiz L y, usándola, definiremos una función

compleja, llamada *la función $\wp$ de Weirstrass*, la cual se denota por $\wp_L$ o por $\wp$ cuando ya no hay posibilidad de confusión. Esta función tendrá las siguientes propiedades:

(1) $\wp$ es analítica en $\mathbb{C} - L$ y tiene polos dobles en los puntos de L.

(2) $\wp$ satisface una ecuación diferencial del tipo $(\wp')^2 = \wp^3 + d\wp + e$. Ya que la última ecuación es la ecuación de una curva elíptica del tipo $y^2 = x^3 + dx + e$ (para un campo de característica distinta de 2 y 3), entonces para cualquier $z \in \mathbb{C} - L$, el punto $(\wp(z), \wp'(z))$ pertenece a la curva elíptica definida por $(\wp')^2 = \wp^3 + d\wp + e$ la cual denotaremos por $\mathbf{E}$.

(3) Dos números complejos z_1 y z_2 en $\mathbb{C} - L$ dan el mismo punto $(\wp(z), \wp'(z))$ en $\mathbf{E}$ si y sólo si $z_1 - z_2 \in L$.

(4) La función que le asocia a cada $z \in \mathbb{C} - L$ el punto $(\wp(z), \wp'(z))$ de $\mathbf{E}$ y le asocia a los puntos de L el punto al infinito ∞ en $\mathbf{E}$ es una biyección entre el grupo cociente $\mathbb{C}/L$ y $\mathbf{E}$.

(5) La correspondencia mencionada en (4) es un isomorfismo de grupos abelianos. En otras palabras si a z_1 le corresponde el punto P y a z_2 le corresponde el punto Q, entonces al punto $z_1 + z_2$ le corresponde el punto $P + Q$.

Una vez enlistadas las propiedades procederemos a ver la demostración de cada una de ellas, para ello necesitaremos definir primeramente la función $\wp$, ya que es la base de todo lo demás.

DEFINICIÓN 3.3.1 ***(Definición de $\wp(z)$)***

Sea $L \subset \mathbb{C}$ una latiz. La función $\wp$ de Weierstrass relativa a la latiz L está definida por la siguiente serie:

$$\wp(z; L) = \frac{1}{z^2} + \sum_{\substack{w \in L \\ w \neq 0}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right) \qquad \text{para toda } z \in \mathbb{C} - L.$$

Una vez definida la función anterior, dado que está definida a partir de una serie de números complejos, primeramente tenemos que ver en qué puntos del plano complejo está definida, lo cual nos lleva a ver los puntos en que la función $\wp$ es convergente. Antes de demostrar esto veamos el siguiente lema.

LEMA 3.3.2 Sea $w_0 \in L$. Definamos $\mathbf{D} = L - \{w_0,\ 0\}$. La serie

$$\sum_{w \in \mathbf{D}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right)$$

converge absolutamente y uniformemente en cualquier subconjunto compacto de $\mathbb{C} - \mathbf{D}$.

DEMOSTRACIÓN.

Para demostrar la convergencia uniforme de la serie tenemos que probar que para cualquier punto $z_0 \in \mathbb{C} - \mathbf{D}$, existe una vecindad $U \subset \mathbb{C} - \mathbf{D}$ de z_0 tal que la serie

$$\sum_{w \in \mathbf{D}} \frac{1}{(z-w)^2} - \frac{1}{w^2}$$

converge absolutamente en U.

Y para esto basta encontrar una vecindad $U \subset \mathbb{C} - \mathbf{D}$ de z_0 y una serie convergente de números positivos $\sum_{w \in \mathbf{D}} M_w$ tal que

$$\left| \frac{1}{(z-w)^2} - \frac{1}{w^2} \right| \leqslant M_w,$$

para toda $z \in U$.

Tomemos $\epsilon > 0$ tal que $\overline{B_\epsilon(z_0)} \cap \mathbf{D} = \emptyset$ y $\epsilon < 1$. Tal ϵ existe porque $\mathbf{D}$ es cerrado en $\mathbb{C}$. Aseguramos que $U = B_\epsilon(z_0)$ tiene la propiedad deseada.

Vamos a dividir al conjunto $\mathbf{D}$ en dos subconjuntos. Definamos

$$\begin{aligned} A &= \{w \in \mathbf{D} :\ |w| \leqslant 2(|z_0| + 1)\} \\ B &= \{w \in \mathbf{D} :\ |w| > 2(|z_0| + 1)\}. \end{aligned}$$

Además como z_0 es fijo, A es el conjunto de puntos de $\mathbf{D}$ que caen en un disco (fijo) por lo que A es finito.

Dada $w \in A$ notemos que la función

$$\frac{1}{(z-w)^2} - \frac{1}{w^2}$$

es una función bien definida y analítica en el conjunto compacto $\overline{U}$ por lo que alcanza su máximo valor y entonces existe $M_w \in \mathbb{R}^+$ tal que

$$\left| \frac{1}{(z-w)^2} - \frac{1}{w^2} \right| \leqslant M_w,$$

para toda $z \in \overline{U}$.

Ahora buscaremos los números de la forma M_w para $w \in B$.

Fijemos $w \in B$. Entonces $|w| > 2(|z_0| + 1)$. Dada $z \in \overline{U}$, $|z| - |z_0| \leqslant |z - z_0| \leqslant \epsilon < 1$. Así que $|z| < 1 + |z_0| < \frac{|w|}{2}$. De modo que $2|z| < |w|$ para toda $z \in \overline{U}$.

Dada $z \in \overline{U}$, notemos que

$$\begin{aligned} \left| \frac{1}{(z-w)^2} - \frac{1}{w^2} \right| &= \left| \frac{w^2 - (z-w)^2}{w^2(z-w)^2} \right| = \left| \frac{w^2 - z^2 + 2zw - w^2}{w^2(z-w)^2} \right| \\ &= \left| \frac{z(2w-z)}{w^2(z-w)^2} \right| = \left| \frac{z}{w^2} \right| \left| \frac{2w-z}{(z-w)^2} \right| \end{aligned}$$

y como $|z_1 - z_2| \leqslant |z_1| + |z_2|$ para cualesquiera números complejos z_1 y z_2, entonces

$$\left| \frac{1}{(z-w)^2} - \frac{1}{w^2} \right| = \left| \frac{z}{w^2} \right| \left| \frac{2w-z}{(z-w)^2} \right| \leqslant \left| \frac{z}{w^2} \right| \left(\frac{|2w| + |z|}{|(z-w)^2|} \right)$$

Ahora bien como $|z| < \frac{|w|}{2}$ tenemos que:

$$\begin{aligned} \left| \frac{1}{(z-w)^2} - \frac{1}{w^2} \right| &\leqslant \left| \frac{z}{w^2} \right| \left(\frac{|2w| + |z|}{|(z-w)^2|} \right) < \left| \frac{z}{w^2} \right| \left(\frac{|2w| + |\frac{w}{2}|}{|(z-w)^2|} \right) \\ &= \left| \frac{z}{w^2} \right| \left(\frac{4|w| + |w|}{2|(z-w)^2|} \right) \end{aligned}$$

y entonces

$$\left|\frac{1}{(z-w)^2}-\frac{1}{w^2}\right| < \left|\frac{z}{w^2}\right|\left(\frac{5|w|}{2|(z-w)^2|}\right) = \left|\frac{z}{w^2}\right|\left(\frac{5|w|}{2|(z+(-w))^2|}\right)$$

Por otro lado cuando $|z_1| > |z_2|$ tenemos que $|z_1| - |z_2| \leqslant |z_1 + z_2|$, por lo que $\frac{1}{|z_1+z_2|} \leqslant \frac{1}{|z_1|-|z_2|}$. De lo anterior, como $|z| < |w|$, entonces:

$$\left|\frac{1}{(z-w)^2}-\frac{1}{w^2}\right| < \left|\frac{5z}{2w^2}\right|\left(\frac{|w|}{|(z+(-w))^2|}\right) \leqslant \left|\frac{5z}{2w^2}\right|\left(\frac{|w|}{\big(|-w|-|z|\big)^2}\right)$$

Además como $2|z| < |w|$, entonces $|z| < \frac{|w|}{2}$, de donde $\frac{|w|}{2} < |w| - |z|$, por lo que $\frac{1}{|w|-|z|} < \frac{2}{|w|}$. Tomando en cuenta esto último y el hecho de que $|-w| = |w|$ obtenemos:

$$\begin{aligned}\left|\frac{1}{(z-w)^2}-\frac{1}{w^2}\right| &< \left|\frac{5z}{2w^2}\right|\left(\frac{|w|}{\big(|-w|-|z|\big)^2}\right) = \left|\frac{5z}{2w^2}\right|\left(\frac{|w|}{\big(|w|-|z|\big)^2}\right) \\ &< \left|\frac{5z}{2w^2}\right|\left(\frac{2}{|w|}\right)^2|w|\end{aligned}$$

simplificando, finalmente obtenemos

$$\left|\frac{1}{(z-w)^2}-\frac{1}{w^2}\right| < \frac{10|z|}{|w|^3} \leqslant \frac{10(|z_0|+1)}{|w|^3}$$

Ahora bien, como sabemos que z_0 es fija entonces únicamente nos faltaría acotar $|w|^{-3}$.

Anteriormente vimos que toda latiz L tiene un par de generadores, digamos que en este caso son w_1 y w_2, entonces cada $w \in L$ se escribe en la forma $w = nw_1 + mw_2$ donde n, $m \in \mathbb{Z}$. Si tomamos la función

$$f(p) = Re(p)w_1 + Im(p)w_2$$

con $p \in \mathbb{C}$, podemos notar que esta función es continua. Por otro lado, como w_1 y w_2 son generadores de L, también serán generadores de $\mathbb{C}$ (pensado como espacio vectorial), es decir, cualquier $q \in \mathbb{C}$ lo podemos escribir como

$q = aw_1 + bw_2$ para algún a y algún b en $\mathbb{R}$, de lo cual podemos decir que la función inversa de f es

$$f^{-1}(q) = f^{-1}(aw_1 + bw_2) = a + ib$$

la cual también es una función continua. Ahora bien, si nos fijamos en las funciones

$$\Big|\big(Re \ \circ \ f^{-1}\big)(q)\Big| \quad \text{y}$$
$$\Big|\big(Im \ \circ \ f^{-1}\big)(q)\Big|$$

éstas tienen como contradominio a los números reales además de que son continuas, esto último ya que tanto $f^{-1}(q)$, $Re(q)$, $Im(q)$ como $|q|$ son continuas. Con lo anterior, si tomamos la función

$$\phi(q) = \Big|\big(Re \ \circ \ f^{-1}\big)(q)\Big| + \Big|\big(Im \ \circ \ f^{-1}\big)(q)\Big|$$

ésta también será continua y tendrá como contradominio a $\mathbb{R}$. Cuando tomamos la región

$$S = \{z' \in \mathbb{C} : |z'| = 1\}$$

podemos notar que es un compacto y al ser ϕ continua, entonces tenemos que debe existir un $M \in \mathbb{R}$ tal que $M > 0$ y además satisface que

$$\phi(z') < M \quad \text{para toda } z' \in S$$

Si hacemos $\delta = \frac{1}{M}$, a continuación veremos que

$$\frac{1}{|w|} \leqslant \frac{1}{\delta(|n| + |m|)}$$

para toda $w \in L - \{0\}$ con $w = nw_1 + mw_2$.

Entonces, si tomamos

$$z = \frac{w}{|w|} = \frac{n}{|w|}w_1 + \frac{m}{|w|}w_2$$

entonces $|z| = 1$ por lo que $z \in S$. Así $\phi(z) < M$, es decir,

$$|\big(Re \circ f^{-1}\big)(z)| + |\big(Im \circ f^{-1}\big)(z)| = |Re\big(f^{-1}(z)\big)| + |Im\big(f^{-1}(z)\big)| < M,$$

pero

$$f^{-1}(z) = f^{-1}\left(\frac{w}{|w|}\right) = f^{-1}\left(\frac{n}{|w|}w_1 + \frac{m}{|w|}w_2\right) = \frac{n}{|w|} + i\frac{m}{|w|},$$

por lo que

$$|Re\big(f^{-1}(z)\big)| + |Im\big(f^{-1}(z)\big)| = \left|Re\left(\frac{n}{|w|} + i\frac{m}{|w|}\right)\right| + \left|Im\left(\frac{n}{|w|} + i\frac{m}{|w|}\right)\right|,$$

así

$$\left|Re\left(\frac{n}{|w|} + i\frac{m}{|w|}\right)\right| + \left|Im\left(\frac{n}{|w|} + i\frac{m}{|w|}\right)\right| = \left|\frac{n}{|w|}\right| + \left|\frac{m}{|w|}\right| = \left|\frac{n}{w}\right| + \left|\frac{m}{w}\right| < M,$$

de donde se sigue que

$$|n| + |m| < M|w|,$$

de donde finalmente obtenemos

$$\frac{1}{|w|} \leqslant \frac{M}{|n| + |m|} = \frac{1}{\delta(|n| + |m|)}.$$

Debemos recordar que el caso que estamos analizando es cuando $w \in B$, pero esta hipótesis no la usamos para encontrar la última ecuación, en sí lo único que necesitaríamos es que tanto m como n sean distintas de cero. Por lo anterior podemos hacer la siguiente observación.

OBSERVACIÓN 3.3.3 Sea L una latiz con generadores w_1 y w_2. Entonces existe un número real $\delta > 0$, tal que para todo $w \in L - \{0\}$ satisface

$$\frac{1}{|w|} \leqslant \frac{1}{\delta(|n| + |m|)}$$

en donde n y m son números en $\mathbb{Z}$ tales que $w = nw_1 + mw_2$.

Continuando con nuestra demostración, recordemos que obtuvimos la desigualdad

$$\left|\frac{1}{(z-w)^2} - \frac{1}{w^2}\right| < \frac{10(|z_0| + 1)}{|w|^3}.$$

Además por la última observación tenemos que

$$\frac{1}{|w|} \leqslant \frac{1}{\delta(|n|+|m|)}$$

con lo anterior obtenemos

$$\left|\frac{1}{(z-w)^2} - \frac{1}{w^2}\right| < \frac{10(|z_0|+1)}{|w|^3} < \frac{10\beta}{\delta^3(|n|+|m|)^3},$$

donde $\beta = |z_0|+1$. Por tanto, para $w \in B$ podemos hacer

$$M_w = \frac{10\beta}{\delta^3(|n|+|m|)^3}.$$

Una vez que hemos encontrado los M_w tanto para A como para B sólo nos faltaría ver que la serie $\sum_{w\in\mathbf{D}} M_w$ converge. Como A es finito, bastará mostrar que la serie

$$\sum_{\substack{(n,m)\in\mathbb{Z}\times\mathbb{Z}\\ nw_1+mw_2\in B}} \frac{10\beta}{\delta^3(|n|+|m|)^3}$$

converge, la notación de la última suma se debe a que en ésta, ya no podemos hacer las sumas variando w, ya que w no aparece en los terminos de la suma, sin embargo, podemos cambiarlo por la suma sobre las parejas (n,m) en $\mathbb{Z}\times\mathbb{Z}$ que cumplen con que $nw_1+mw_2 \in B$, en si los terminos de ésta serie son tantos como los terminos de la serie $\sum_{w\in B} M_w$. Finalmente basta ver que la serie

$$\sum_{\substack{(n,m)\in\mathbb{Z}\times\mathbb{Z}\\ |n|+|m|\neq 0}} \frac{10\beta}{\delta^3(|n|+|m|)^3}$$

converge. Dada $(n,m) \in (\mathbb{Z}\times\mathbb{Z})\backslash\{(0,0)\}$, hagamos $N = |n|+|m|$. Cuando tomamos n entre 1 y $N-1$, podemos encontrar un número m en los naturales que cumpla con $N = |n|+|m|$, pero tomando en cuenta el valor absoluto por cada pareja de números n y m encontrados de esta manera podemos notar que habrá otros 3 pares de números en $\mathbb{Z}$ que también cumplirán con $N = |n|+|m|$, éstos serían $-n$ y m, n y $-m$ y finalmente $-n$ y $-m$, con lo que tendremos $4(N-1)$ pares de números que cumplen la ecuación de N.

Pero también cumplirán las parejas N con 0, $-N$ con 0, 0 con N y 0 con $-N$, con lo que tendremos otros 4 pares. De tal modo que hay $4N$ pares de números n, m que cumplen la ecuación de N. Por lo que

$$\sum_{\substack{(n,m)\in\mathbb{Z}\times\mathbb{Z}\\ |n|+|m|\neq 0}} \frac{1}{\delta^3(|n|+|m|)^3} = \sum_{N\in\mathbb{N}} \frac{4N}{(\delta N)^3} = \frac{4}{\delta^3}\sum_{N\in\mathbb{N}} \frac{1}{N^2},$$

y como sabemos que $\sum \frac{1}{N^2}$ es una serie convergente y además 4 y δ^3 son constantes, entonces $\frac{4}{\delta^3}\sum \frac{1}{N^2}$ también es convergente por lo que

$$\sum_{\substack{(n,m)\in\mathbb{Z}\times\mathbb{Z}\\ |n|+|m|\neq 0}} \frac{1}{\delta^3(|n|+|m|)^3} < \infty.$$

Así finalmente obtendremos

$$\sum_{\substack{(n,m)\in\mathbb{Z}\times\mathbb{Z}\\ |n|+|m|\neq 0}} \frac{10\beta}{\delta^3(|n|+|m|)^3} < \infty.$$

Por tanto la serie

$$\sum_{w\in\mathbf{D}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2}\right)$$

converge absolutamente en U para toda $z \in \mathbb{C} - \mathbf{D}$. ■

Una vez visto el lema anterior podemos demotrar el lema que queremos sobre $\wp(z)$.

LEMA 3.3.4 La serie $\wp(z)$ converge absolutamente y uniformemente en cualquier subconjunto compacto de $\mathbb{C} - L$.

DEMOSTRACIÓN.

Como en el lema anterior, nos bastará con probar que para cualquier punto $z_0 \in \mathbb{C} - L$, existe una vecindad $U \subset \mathbb{C} - L$ de z_0 tal que la serie

$$\frac{1}{z^2} + \sum_{\substack{w\in L\\ w\neq 0}} \frac{1}{(z-w)^2} - \frac{1}{w^2}$$

converge absolutamente en U.

Y para esto basta encontrar una vecindad $U \subset \mathbb{C} - L$ de z_0 y una serie convergente de números positivos $\sum_{\substack{w \in L \\ w \neq 0}} M_w$ tal que

$$\left| \frac{1}{(z-w)^2} - \frac{1}{w^2} \right| \leqslant M_w,$$

para toda $z \in U$.

En el lema anterior teníamos que dada $w_0 \in L$ y $z_0 \in \mathbb{C} - \mathbf{D}$ (donde $\mathbf{D} = L - \{w_0, 0\}$ podíamos tomar ϵ_1 y encontrar M_w tal que

$$\left| \frac{1}{(z-w)^2} - \frac{1}{w^2} \right| \leqslant M_w,$$

para cada $w \in \mathbf{D}$ (con $\mathbf{D} = L - \{w_0, 0\}$) y toda $z \in U_1$ ($U_1 = B_{\epsilon_1}(z_0)$). En donde la serie $\sum_{w \in \mathbf{D}} M_w$ es una serie convergente.

De lo anterior, dada $z_0 \in \mathbb{C} - L$ tomemos $\epsilon < \epsilon_1$ tal que $\overline{B_\epsilon(z_0)} \cap L = \emptyset$. Sea $U = B_\epsilon(z_0)$. Notemos que como $\epsilon < \epsilon_1$, entonces $U \subset U_1$. Además las M_w antes mencionadas cumplen que

$$\left| \frac{1}{(z-w)^2} - \frac{1}{w^2} \right| \leqslant M_w,$$

para cada $w \in \mathbf{D}$ y toda $z \in U$. Por lo que sólo nos faltará encontrar las M_w correspondientes a z^{-2} (ésta M_w la denotaremos por M_0) y a $(z-w_0)^{-2} - w_0^{-2}$.

Como 0 y w_0 están en L, entonces tanto z^{-2} como $(z-w_0)^{-2} - w_0^{-2}$, son funciones bien definidas y analíticas en $\mathbb{C} - L$. En particular también son analíticas en $\overline{U}$, el cual es un compacto, por lo que alcanzan su valor máximo y mínimo. Por lo que existen M_0 y M_w en $\mathbb{R}^+$ tales que

$$\left| \frac{1}{z^2} \right| < M_0 \qquad y \qquad \left| \frac{1}{(z-w_0)^2} - \frac{1}{(w_0)^2} \right| < M_{w_0}$$

Por lo que

$$\left| \tfrac{1}{z^2} \right| + \left| \tfrac{1}{(z-w_0)^2} - \tfrac{1}{(w_0)^2} \right| + \sum_{w \in \mathbf{D}} \left| \tfrac{1}{(z-w)^2} - \tfrac{1}{(w)^2} \right|$$

$$< M_0 + M_{w_0} + \sum_{w \in \mathbf{D}} M_w = \sum_{w \in L} M_w.$$

Pero como ya habíamos visto $\sum_{w\in\mathbf{D}} M_w$ es convergente, por lo que $\sum_{w\in L} M_w$ también es convergente. Así la serie

$$\frac{1}{z^2}+\sum_{\substack{w\in L\\ w\neq 0}}\left(\frac{1}{(z-w)^2}-\frac{1}{(w)^2}\right)$$

converge absolutamente en U, que es lo que queríamos demostrar. ■

Con lo anterior ya mostramos en qué puntos está definida $\wp$. Derivado del lema anterior tenemos el siguiente corolario.

COROLARIO 3.3.5 La función $\wp$ es analítica en $\mathbb{C}-L$, es decir, existe $\wp'$ que está definida por la serie

$$\sum_{w\in L}\frac{-2}{(z-w)^3} \quad \text{para todo} \quad z\in\mathbb{C}-L$$

y además esta serie es convergente.

Este corolario se deriva del hecho de que toda serie absolutamente convergente en una región $D\subset\mathbb{C}$, es analítica en D, además de que existe la derivada de esta serie la cual se obtiene derivando término a término los sumandos de la serie $\wp(z)$.[1] Por la misma razón tenemos el siguiente corolario.

COROLARIO 3.3.6 Sea $w_0\in L$. Definamos $\mathbf{D}=L-\{w_0,0\}$. La serie

$$\sum_{w\in\mathbf{D}}\left(\frac{1}{(z-w)^2}-\frac{1}{(w)^2}\right)$$

es analítica en todo $z\in\mathbb{C}-\mathbf{D}$.

Con lo que ya hemos demostrado podemos empezar a ver las propiedades que tienen $\wp$ y $\wp'$. Primeramente veremos que $\wp$ es una función par y que $\wp'$ es una función impar, además de ver que para toda $w\in L$ y toda $z\in\mathbb{C}-L$,

$$\begin{aligned}\wp'(z) &= \wp'(z+w)\\ \wp(z) &= \wp(z+w)\end{aligned}$$

[1] Teorema 2 ubicado en la página 38 de [**?**].

LEMA 3.3.7 $\wp(z)$ es una función par y $\wp'(z)$ es una función impar. Además para toda $w \in L$ se cumple

$$\begin{aligned} \wp'(z) &= \wp'(z+w) \qquad \text{para toda } \ z \in \mathbb{C} - L \\ \wp(z) &= \wp(z+w) \qquad \text{para toda } \ z \in \mathbb{C} - L \end{aligned}$$

DEMOSTRACIÓN.

Para demostrar que $\wp$ es una función par debemos demostrar que para toda $z \in \mathbb{C} - L$

$$\wp(z) = \wp(-z)$$

para ello debemos tomar en cuenta que $(z-w)^2 = (-z+w)^2$ y $w^2 = (-w)^2$ para toda $z \in \mathbb{C} - L$ y toda $w \in L$. Con esto tenemos que

$$\begin{aligned} \wp(z) &= \frac{1}{z^2} + \sum_{\substack{w \in L \\ w \neq 0}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right) = \frac{1}{z^2} + \sum_{\substack{w \in L \\ w \neq 0}} \left(\frac{1}{(-z+w)^2} - \frac{1}{w^2} \right) \\ &= \frac{1}{(-z)^2} + \sum_{\substack{w \in L \\ w \neq 0}} \left(\frac{1}{\Big(-z-(-w)\Big)^2} - \frac{1}{(-w)^2} \right) \end{aligned}$$

Como a final de cuentas, $w \in L$ si y sólo si $-w \in L$, entonces podemos hacer el cambio de variable $-w = w'$, de tal manera que la última ecuación quedará como

$$\begin{aligned} \wp(z) &= \frac{1}{(-z)^2} + \sum_{\substack{w' \in L \\ w' \neq 0}} \left(\frac{1}{(-z-w')^2} - \frac{1}{(w')^2} \right) \\ &= \wp(-z) \end{aligned}$$

Con lo cual obtenemos que $\wp(z) = \wp(-z)$. Ahora bien, para ver que $\wp'(z)$ es impar simplemente derivamos de ambos lados de la ecuación $\wp(z) = \wp(-z)$.

Ahora demostraremos que $\wp'(z) = \wp'(z+w_0)$ para toda z en $\mathbb{C} - L$ y toda $w_0 \in L$. Por la definición de $\wp'$ tenemos que para toda $z \in \mathbb{C} - L$ y toda $w_0 \in L$

$$\wp'(z+w_0) = -2 \sum_{w \in L} \frac{1}{(z+w_0-w)^3}$$

Debemos notar que si tomamos $w_0 \in L$, entonces $w \in L$ si y sólo si $w_0 - w \in L$, por lo que podemos hacer el cambio de variable $w' = w_0 - w$, con lo que obtenemos que

$$\begin{aligned} \wp'(z+w_0) &= -2\sum_{w\in L}\frac{1}{(z+w_0-w)^3} = -2\sum_{w'\in L}\frac{1}{(z-w')^3} \\ &= \wp'(z) \end{aligned}$$

Con lo cual demostramos lo que queríamos. Ahora bien para demostrar que $\wp(z) = \wp(z+w_0)$ para toda $w_0 \in L$ y toda $z \in \mathbb{C} - L$ será suficiente con demostrar los casos en que $w_0 = nw_1$ y $w_0 = nw_2$ para toda $n \in \mathbb{Z}$, esto por que todo w_0 se puede escribir de la forma $w_0 = nw_1 + mw_2$, entonces si demostramos que $\wp(z) = \wp(z+nw_1)$ y $\wp(z) = \wp(z+nw_2)$ para toda $n \in \mathbb{Z}$ tendremos que

$$\wp(z+w_0) = \wp(z+nw_1+mw_2) = \wp(z+nw_1) = \wp(z)$$

ya que ni $z+nw_1$ ni z están en L. Primero analicemos el caso en que $n \in \mathbb{N}$, como se trata de naturales lo haremos por inducción.

Demostremos primero cuando $n = 1$, es decir, $w_0 = w_1$. Para ello construyamos la función $f(z) = \wp(z+w_1) - \wp(z)$. De la función f podemos decir que como $\wp$ es una función analítica en $\mathbb{C}-L$, entonces f es analítica en $\mathbb{C}-L$, y además esta función tiene como derivada $f'(z) = \wp'(z+w_1) - \wp'(z)$, pero por lo último que demostramos $f'(z)$ es 0 en cualquier punto $z \in \mathbb{C}-L$, es decir, $f'(z) = 0$ para toda $z \in \mathbb{C}-L$ y como $\mathbb{C}-L$ es conexo la función $f(z)$ tiene que ser una función constante. Además como $-w_1/2 \notin L$, entonces $f(z)$ evaluada en $-w_1/2$ es

$$f(-w_1/2) = \wp\left(-\frac{w_1}{2}+w_1\right) - \wp\left(-\frac{w_1}{2}\right)$$

pero ya vimos que $\wp$ es una función par por lo que

$$\begin{aligned} f(-w_1/2) &= \wp\left(\frac{w_1}{2}\right) - \wp\left(-\frac{w_1}{2}\right) \\ &= 0 \end{aligned}$$

Por lo que la constante que buscamos es 0. Así que $f(z) = 0$, entonces $\wp(z+w_1) = \wp(z)$ para toda $z \in \mathbb{C} - L$.

Para hacer el paso inductivo, supongamos que $\wp\big(z+(n-1)w_1\big)=\wp(z)$ para toda $z\in\mathbb{C}-L$. Demostremos que $\wp(z+nw_1)=\wp(z)$. Notemos que $z+nw_1=z+(n-1)w_1+w_1$, en donde, como ya vimos $z+(n-1)w_1\notin L$ y ya que $\wp(z+w_1)=\wp(z)$ para todo $z\in\mathbb{C}-L$, así

$$\wp(z+nw_1)=\wp(z+(n-1)w_1+w_1)=\wp\big(z+(n-1)w_1\big)$$

y por nuestra suposición tenemos que

$$\wp(z+nw_1)=\wp\big(z+(n-1)w_1\big)=\wp(z)$$

por lo que

$$\wp(z+nw_1)=\wp(z)$$

es válido para toda $n\in\mathbb{N}$. Ahora si tomamos $n\in\mathbb{Z}^-$, $-n$ pertenece a los naturales. Por lo que ya demostramos (aplicado a $z+nw_1$), tenemos que $\wp((z+nw_1)+(-nw_1))=\wp(z+nw_1)$, así que $\wp(z+nw_1)=\wp(z)$. Por tanto la igualdad $\wp(z+nw_1)=\wp(z)$ se cumple para todo $n\in\mathbb{Z}$.

Análogamente podemos demostrar lo mismo con w_2. Con lo dicho al principio finalmente obtenemos que $\wp(z+w_0)=\wp(z)$. Lo anterior quiere decir que la función $\wp$ manda a z y a $z+w_0$ al mismo punto, y como w_0 era cualquiera en la latiz, entonces dada $z\in\mathbb{C}-L$, a todos los puntos del conjunto:

$$\{z+w : w\in L\}$$

la función $\wp$ los manda al mismo punto.

Con esto concluimos la demostración del lema. ■

Con lo anterior podemos saber que es lo que ocurre con $\wp$ en los puntos $z\in\mathbb{C}-L$, sin embargo, todavía nos faltaría determinar que ocurre en los puntos w que están en L. Para ello tomemos $w_0\in L-\{0\}$. La función z^{-2} es una función analítica en $\mathbb{C}-\{0\}$ y por el corolario 3.3.6 tenemos que

$$\sum_{w\in\mathbf{D}}\left(\frac{1}{(z-w)^2}-\frac{1}{w^2}\right)$$

es analítica en todo $z\in\mathbb{C}-\mathbf{D}$ (donde $\mathbf{D}=L-\{w_0,0\}$). Por lo que la serie

$$\frac{1}{z^2}+\sum_{w\in\mathbf{D}}\left(\frac{1}{(z-w)^2}-\frac{1}{w^2}\right)$$

es analítica en $\mathbb{C} - L$ y también en w_0. En particular, nos interesa que la serie es analítica en una vecindad de w_0. Exactamente, es analítica en el disco de radio R con centro en w_0 ($B_R(w_0)$), donde $R = min\{|w_1|, |w_2|\}$ (recordemos que w_1 y w_2 son los generadores de L). Ya que es analítica en esta vecindad, entonces el teorema de Taylor[2] nos garantiza que existen A_i con $i = 1, 2, \ldots$ tales que

$$\frac{1}{z^2} + \sum_{w \in \mathbf{D}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right) = \sum_{i=0}^{\infty} \frac{A_i}{i!} (z - w_0)^i$$

para toda $z \in B_R(w_0)$. Además tenemos que

$$\frac{1}{(z-w_0)^2} - \frac{1}{(w_0)^2}$$

es analítica en $\mathbb{C} - \{w_0\}$, en particular, en $B_R(w_0) - \{w_0\}$. De tal modo que

$$\begin{aligned} \wp(z) &= \left(\frac{1}{(z-w_0)^2} - \frac{1}{(w_0)^2} \right) + \frac{1}{z^2} + \sum_{w \in \mathbf{D}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right) \\ &= \left(\frac{1}{(z-w_0)^2} - \frac{1}{(w_0)^2} \right) + \sum_{i=0}^{\infty} \frac{A_i}{i!} (z - w_0)^i \end{aligned}$$

es analítica en $B_R(w_0)$ salvo en w_0. Pero el lado derecho de la igualdad no es mas que la serie de Laurent correspondiente a $\wp$ alrededor de w_0.

Recordemos que una función tiene un polo de orden N, si en la parte principal del desarrollo en serie de Laurent de dicha función alrededor de un punto z_0, los coeficientes de los términos correspondientes a $(z - z_0)^{-k}$ son 0 para todo $k \in \mathbb{N}$ con $k > N$. Además, de que el coeficiente del término que contiene a $(z - z_0)^{-N}$ es distinto de 0. Así, como la parte principal de la serie de Laurent de $\wp$ alrededor de w_0 es $(z - w_0)^{-2}$, tenemos que $\wp$ tiene un polo de orden 2 alrededor de w_0.

Análogmanete, podemos ver que $\wp$ tiene un polo de orden 2 alrededor del 0. De lo anterior podemos deducir el siguiente teorema.

[2]Teorema 3 en la página 179 de [ah]

TEOREMA 3.3.8 La función $\wp(z)$ tiene polos dobles en los puntos de L.

Uno de los problemas que se tienen por estar $\wp$ definida como una serie, es lo complicado que resulta calcular expresiones simples y apropiadas para las funciones

$$\wp^3(z) = \left(\frac{1}{z^2} + \sum_{\substack{w\in L\\ w\neq 0}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2}\right)\right)^3$$

$$\text{y} \quad \left(\wp'(z)\right)^2 = \left(-2\sum_{w\in L} \frac{1}{(z-w)^3}\right)^2.$$

Para poder hacer esto se introducen nuevas funciones como la de la siguiente definición.

DEFINICIÓN 3.3.9 Sea L una latiz, entonces definimos la serie de Eisenstein de peso $2k$ (con $k \geq 2$) como

$$G_{2k}(L) = \sum_{\substack{w\in L\\ w\neq 0}} w^{-2k}$$

Antes de utilizar esta serie será importante analizar si esta serie es convergente, para ello veamos el siguiente teorema.

TEOREMA 3.3.10 Para cada latiz L la serie de Eisenstein G_{2k} es absolutamente convergente para toda $k \in \mathbb{N}$

DEMOSTRACIÓN. Para demostrar esto necesitamos que la serie

$$\sum_{\substack{w\in L\\ w\neq 0}} |\omega^{-2k}|$$

sea convergente para $k \geq 2$, para ello recordemos que en la observación 3.3.3 dentro de la demostración del teorema 3.3.2 obtuvimos el siguiente resultado.

$$\text{Existe } c \in \mathbb{R}^+ \text{ tal que para toda } w \in L - \{0\}, \quad \frac{1}{|w|} \leqslant \frac{1}{c(|n| + |m|)},$$

en donde recordemos que $|w| = |nw_1 + mw_2|$ con $n, m \in \mathbb{Z}$ y $|n|+|m| \neq 0$, por lo que si sumamos sobre $w \in L - \{0\}$ en el lado izquierdo de la desigualdad, entonces las sumas correrán sobre n y m en el lado derecho con la condición de que $|n| + |m| \neq 0$, esto es:

$$\sum_{\substack{w \in L \\ w \neq 0}} \frac{1}{|w|^{2k}} \leqslant \sum_{\substack{n,m \in \mathbb{Z} \\ |n|+|m| \neq 0}} \frac{1}{\big(c(|n| + |m|)\big)^{2k}},$$

si hacemos $N = |n| + |m|$ tendremos 4N parejas de números n y m que van a satisfacer está condicion por lo que

$$\sum_{\substack{w \in L \\ w \neq 0}} \frac{1}{|w|^{2k}} \leqslant \sum_{\substack{n,m \in \mathbb{Z} \\ |n|+|m| \neq 0}} \frac{1}{\big(c(|n| + |m|)\big)^{2k}} = \sum_{N \in \mathbb{N}} \frac{4N}{\big(cN\big)^{2k}} = \frac{4}{c^{2k}} \sum_{N \in \mathbb{N}} N^{-2k+1}$$

y como $\sum_{N \in \mathbb{N}} N^{-j}$ es convergente para cualquier $j \in \mathbb{N}$ tal que $j \geqslant 2$, entonces $\sum_{N \in \mathbb{N}} N^{-2k+1}$ es convergente para toda $k \in \mathbb{N}$ tal que $k \geq 2$, ademas como $4c^{-2k}$ es una constante entonces

$$\frac{4}{c^{2k}} \sum_{N \in \mathbb{N}} N^{-2k+1} \qquad \text{para toda } k \in \mathbb{N}$$

es convergente por lo que

$$G_{2k} = \sum_{\substack{w \in L \\ w \neq 0}} \frac{1}{|w|^{2k}} \qquad \text{para toda } k \in \mathbb{N}$$

es convergente, que es lo que queríamos demostrar. ∎

Ya que la series G_{2k} son convergentes podemos enlistar las siguientes igualdades, sus pruebas son complicadas y quedan fuera del alcance de este trabajo, sin embargo, usaremos estas expresiones. [3]

$$\begin{aligned}
\wp\prime(z) &= -\frac{2}{z^3} + 6G_4 z + 20G_6 z^3 + 42G_8 z^5 + ..., \\
\big(\wp'(z)\big)^2 &= \frac{4}{z^6} - 24G_4 \frac{1}{z^2} - 80G_6 + (36(G_4)^2 - 168G_8)z^2 + ..., \\
\big(\wp(z)\big)^2 &= \frac{1}{z^4} + 6G_4 + 10G_6 z^2 + ...,
\end{aligned}$$

[3]Desafortunadamente no pude encontrar demostraciones de estas ecuaciones y desconozco si hay alguna prueba, las ecuaciones utilizadas aquí están escritas como en [**?**] página 275.

$$\begin{aligned}\big(\wp(z)\big)^3 &= \frac{1}{z^6} + 9G_4\frac{1}{z^2} + 15G_6 + (21G_8 + 27(G_4)^2)z^2 + ...,\\ \wp(z) &= \frac{1}{z^2} + 3G_4z^2 + 5G_6z^4 + 7G_8z^6 + ...,\end{aligned}$$

Cada una de las series anteriores es convergente, ya que el producto de series absolutamente convergentes es una una serie absolutamente convergente[4] y tanto $\wp$ como $\wp'$ lo son. Con esto definamos la función $f(z)$ como sigue:

$$f(z) = \big(\wp'(z)\big)^2 - 4\big(\wp(z)\big)^3 + 60G_4\wp(z) + 140G_6$$

sustituyendo, obtenemos

$$\begin{aligned}f(z) &= \frac{4}{z^6} - 24G_4\frac{1}{z^2} - 80G_6 + (36(G_4)^2 - 168G_8)z^2 + ...\\ &\quad -4\Big[\frac{1}{z^6} + 9G_4\frac{1}{z^2} + 15G_6 + (21G_8 + 27(G_4)^2)z^2 + ...\Big]\\ &\quad +60G_4\Big[\frac{1}{z^2} + 3G_4z^2 + 5G_6z^4 + 7G_8z^6 + ...\Big]\\ &\quad +140G_6\\ &= \left(\frac{4}{z^6} - \frac{4}{z^6}\right) + (60G_4 - 36G_4 - 24G_4)\frac{1}{z^2} - 80G_6 - 60G_6 + 140G_6\\ &\quad +\left(36(G_4)^2 - 168G_8 - 4\Big(21G_8 + 27(G_4)^2\Big) + 180(G_4)^2\right)z^2 + ...\\ f(z) &= \Big(108(G_4)^2 - 252G_8\Big)z^2 + ...\end{aligned}$$

En esta última expresión, tenemos a f expresada como una serie de potencias alrededor del cero. Si $z \in \mathbb{C} - L$, esta serie es convergente, porque cada una de las funciones $(\wp'(z))^2$, $(\wp(z))^3$, $\wp(z)$ estaba dada como una serie absolutamente convergente. Por tanto el radio de convergencia de la serie que define a f es infinito. Así que f es analítica en $\mathbb{C}$.

Por otro lado recordemos que

$$\begin{aligned}\wp(z) &= \wp(z+w) \qquad \forall z \in \mathbb{C} - L \;\; y \;\; \forall\, w \in L\\ \wp(z') &= \wp'(z+w) \qquad \forall z \in \mathbb{C} - L \;\; y \;\; \forall\, w \in L,\end{aligned}$$

[4]Teorema 5 en la pág. 240 de [**?**]

por lo que

$$\begin{aligned} \wp(z) &= \wp(z+w) \qquad \forall z \in \mathbb{C} - L \;\; y \;\; \forall\, w \in L \\ \big(\wp(z)\big)^3 &= \big(\wp(z+w)\big)^3 \qquad \forall z \in \mathbb{C} - L \;\; y \;\; \forall\, w \in L \\ \wp(z') &= \wp'(z+w) \qquad \forall z \in \mathbb{C} - L \;\; y \;\; \forall\, w \in L, \end{aligned}$$

entonces

$$\begin{aligned} f(z) &= \big(\wp'(z)\big)^2 - 4\big(\wp(z)\big)^3 + 60G_4\wp(z) + 140G_6 \\ &= \big(\wp'(z+w)\big)^2 - 4\big(\wp(z+w)\big)^3 + 60G_4\wp(z+w) + 140G_6 \\ f(z) &= f(z+w) \qquad \forall z \in \mathbb{C} - L \;\; y \;\; \forall\, w \in L. \end{aligned}$$

Como f es analítica en 0, entonces f también es continua en 0, así

$$f(0) = \lim_{z \to 0} f(z)$$

pero como para todo $z \in \mathbb{C} - L$ tenemos que $f(z) = f(z+w)$, entonces

$$f(0) = \lim_{z \to 0} f(z) = \lim_{z \to 0} f(z+w) = f(w) \quad \forall\, w \in L.$$

Por lo que podemos concluir que

$$f(z) = f(z+w) \quad \forall\, z \in \mathbb{C} \;\; y \;\; \forall\, w \in L.$$

Definimos

$$D = \{z \in \mathbb{C} \;:\; z = kw_1 + jw_2 \quad \text{con} \quad k, j \in [0,1]\},$$

donde w_1, w_2 son los generadores de L. Entonces si buscamos el supremo de $|f|$ en $\mathbb{C}$ éste será igual al supremo de $|f|$ en D, es decir:

$$sup\{|f(z)| \;: z \in \mathbb{C}\} = sup\{|f(z)| \;: z \in D\}$$

Notemos que D es compacto y f es continua en D, de manera que f es acotada en D. Esto implica que f es acotada en $\mathbb{C}$ y como $f(0) = 0$, por el Teorema de Liouville tenemos que la función f es constante, es decir, que $f(z) = 0$ para toda $z \in \mathbb{C}$. Dado que $f(z) = \big(\wp'(z)\big)^2 - 4\big(\wp(z)\big)^3 + 60G_4\wp(z) + 140G_6$ resulta que:

$$f(z) = \big(\wp'(z)\big)^2 - 4\big(\wp(z)\big)^3 + 60G_4\wp(z) + 140G_6 = 0$$

Por tanto

$$\big(\wp'(z)\big)^2 = 4\big(\wp(z)\big)^3 - 60G_4\wp(z) - 140G_6$$

Hemos demostrado el siguiente teorema.

TEOREMA 3.3.11 Dada una latiz L en $\mathbb{C}$,

$$\big(\wp'(z)\big)^2 = 4\big(\wp(z)\big)^3 - 60G_4\wp(z) - 140G_6,$$

para toda $z \in \mathbb{C} - L$

Consideremos la ecuación

$$y^2 = 4x^3 - 4ax + c \quad \text{con } x, y \in \mathbb{C},$$

Aplicando la trasformación dada por:

$$\widetilde{x} = 4^{1/3}x \qquad \widetilde{y} = y,$$

obtenemos la ecuación

$$\widetilde{y}^2 = \widetilde{x}^3 - \frac{4}{4^{\frac{1}{3}}}a\widetilde{x} + c,$$

la cual es la ecuación de una curva elíptica, por lo que $\big(\wp'(z)\big)^2 = 4\big(\wp(z)\big)^3 - 60G_4\wp(z) - 140G_6$ es la ecuación de una curva elíptica transformada, de está manera queda demostrada la propiedad 2 de las curvas elípticas en $\mathbb{C}$ que enunciamos en la página 73.

Antes de ver la propiedad 3 necesitamos ver algunas definiciones y resultados importantes de variable compleja que serán de gran ayuda, en particular veremos algunos resultados del cálculo de residuos, comenzaremos con la siguientes definiciones.

DEFINICIÓN 3.3.12 Sea γ una curva diferenciable a trozos dentro de una región $\Omega \in \mathbb{C}$ y tomemos un punto $a \in \Omega$, tal que γ no pasa por a, entonces definimos el *indíce de el punto a con respecto a la curva* γ por la ecuación:

$$n(\gamma, a) = \frac{1}{2\pi i}\int_\gamma \frac{dz}{z-a}$$

Se puede demostrar que $n(\gamma,\ a)$ siempre es un número entero (lema 1 de [**?**] pag. 115), además, de que el índice de un punto a con respecto a la curva γ también se puede describir como el número de vueltas con orientación que γ da alrededor de a.

DEFINICIÓN 3.3.13 Una curva γ en un conjunto abierto Ω se dice ser *homóloga a cero con respecto a la región* Ω si $n(\gamma, a) = 0$ para todos los puntos en el complemento de Ω. En símbolos esto se escribira como $\gamma \sim 0 \pmod{\Omega}$

DEFINICIÓN 3.3.14 Sea f(z) una una función analítica en una región D excepto quizás en un punto a. Entonces la serie de Laurent de $f(z)$ es de la siguiente forma

$$f(z) = \sum_{-\infty}^{\infty} a_n (z-a)^n,$$

donde esta serie converge en un anillo de la forma

$$0 < |z-a| < r_1.$$

Entonces definimos el residuo de $f(z)$ en el punto a como:

$$Res_{z=a} f(z) = a_{-1}.$$

A partir de estas definiciones, se siguen varios resultados que nos serán de gran utilidad para poder demostrar la propiedad 3. Iniciaremos con el Teorema del residuo.

TEOREMA 3.3.15 (Teorema del residuo)

Sea $f(z)$ analítica excepto para singularidades aisladas[5] a_j en una región $\Omega \in \mathbb{C}$. Entonces

$$\frac{1}{2\pi} \int_\gamma f(z)dz = \sum_j n(\gamma, a_j) Res_{z=a_j} f(z),$$

para cualquier curva γ que sea homóloga a cero en Ω y no pase por ninguno de los puntos a_j.

[5]Puntos para los cuales existe una vecindad en la que, salvo por el mismo punto, f es analítica en dicha vecindad (es decir, un punto a es una singularidad aislada de f, si f es analítica en todo b tal que $b \in B_\delta(a)\backslash\{a\}$ para alguna $\delta \in \mathbb{R}^+$)

Derivado del teorema anterior tenemos el siguiente lema.

LEMA 3.3.16 Si $f(z)$ es analítica en una región $\Omega \in \mathbb{C}$, entonces

$$n(\gamma, a)f(a) = \frac{1}{2\pi\imath}\int_{\gamma}\frac{f(z)}{z-a}dz$$

para cualquier curva γ que sea homóloga a cero en Ω.

Otros conceptos que son importantes de recordar son los de cero y polo, los cuales enunciaremos en las siguientes definiciones.

DEFINICIÓN 3.3.17 Sea f una función definida en $\mathbb{C}$. Diremos que un punto $a \in \mathbb{C}$ es un *cero* de f si $f(a) = 0$. Más generalmente diremos que a es un *cero de orden* h si existe una función $f_h(z)$ que sea analítica y diferente de cero en a (es decir $f_h(a) \neq 0$), tal que

$$f(z) = (z-a)^h f_h(z)$$

DEFINICIÓN 3.3.18 Sea f una función definida en $\mathbb{C}$. Diremos que un punto $a \in \mathbb{C}$ es un *polo* de f si a es una singularidad aislada de f y además

$$\lim_{z\to a}|f(z)| = \infty$$

En general diremos que a es un polo de orden h si existe una función $f_h(z)$ que sea analítica y diferente de cero en a (es decir $f_h(a) \neq 0$), tal que

$$f(z) = (z-a)^{-h} f_h(z)$$

De estas definiciones se pueden deducir varios teoremas importantes sobre ceros y polos en funciones complejas. Cuando una función f tiene un cero de orden h como ya vimos se puede escribir a la función como $f(z) = (z-a)^h f_h(z)$ en donde $f_h(a) \neq 0$. Derivando f obtenemos $f'(z) = h(z-a)^{h-1}f_h(z) + (z-a)^h f_h'(z)$. Así tenemos que

$$\frac{f'(z)}{f(z)} = \frac{h}{z-a} + \frac{f_h'(z)}{f_h(z)}$$

entonces f'/f tiene un polo simple con residuo h.

Si tomamos una función analítica $g(z)$ en $\mathbb{C}$ tal que $g(z) \neq 0$, entonces

$$g(z)\frac{f'(z)}{f(z)} = g(z)\frac{h}{z-a} + g(z)\frac{f_h'(z)}{f_h(z)}$$

tendrá un polo simple en a con residuo $hg(a)$. Análogamente tendremos que si f tiene un polo de orden k en b entonces:

$$\frac{f'(z)}{f(z)} \qquad \text{tendrá un polo simple en } b \text{ con residuo } k$$

$$y \quad g(z)\frac{f'(z)}{f(z)} \qquad \text{tendrá un polo simple en } b \text{ con residuo } kg(a)$$

Derivado de estos resultados y del teorema del residuo se deducen el principio del argumento y su generalización.

TEOREMA 3.3.19 (Principio del argumento)

Si $f(z)$ es analítica en una región $\Omega \in \mathbb{C}$ y $f(z)$ es analítica en Ω con ceros en a_j y polos en b_k, entonces

$$\frac{1}{2\pi\imath}\int_\gamma \frac{f'(z)}{f(z)}dz = \sum_j n(\gamma, a_j) - \sum_k n(\gamma, b_k)$$

Para cualquier curva γ que sea homóloga a cero en una región $\Omega \in \mathbb{C}$ y no pase sobre ningún polo o cero de f.

TEOREMA 3.3.20 (Generalización del principio del argumento)

Sean $g(z)$ y $f(z)$ analíticas en Ω, en donde $f(z)$ tiene ceros en a_j y polos en b_k, entonces

$$\frac{1}{2\pi\imath}\int_\gamma g(z)\frac{f'(z)}{f(z)}dz = \sum_j n(\gamma, a_j)g(a_j) - \sum_k n(\gamma, b_k)g(b_k)$$

Para cualquier curva γ que sea homologa a cero en Ω y no pase sobre ningún polo o cero de f.

Cabe aclarar que cuando los ceros y polos son múltiples, tendrán que ser repetidos en las sumas tantas veces como indique el orden respectivo. En particuar del último teorema tenemos que cuando $n(\gamma, a_j) = n(\gamma, b_k) = 1 \quad \forall\, j, k$ entonces

$$\frac{1}{2\pi\imath}\sum_{\gamma} g(z)\frac{f'(z)}{f(z)}dz = \sum_{j} g(a_j) - \sum_{k} g(b_k)$$

Otro resultado que ocuparemos y que no está relacionado con el cálculo de residuos es el siguiente.

LEMA 3.3.21 Sea f una función definida en $\mathbb{C}$ que cumple con que $f(z) = f(z+a)$, donde a es algún punto en $\mathbb{C}$ y tomemos dos curvas γ_1 y γ_2 tales que

$$\gamma_1,\ \gamma_2 : [c,d] \subset \mathbb{R} \to \mathbb{C}$$

$$\text{y} \quad \gamma_1(t) = \gamma_2(t) + a \qquad \text{para cada } t \in [c,d] \qquad \text{entonces}$$

$$\int_{\gamma_1} f(z)dz = \int_{\gamma_2} f(z)dz$$

mientras las curvas sean recorridas en el mismo sentido. Si son recorridas en sentidos opuestos (es decir, si $\gamma_1(t) = \gamma_2(d - t + c) + a$ tendremos

$$\int_{\gamma_1} f(z)dz = -\int_{\gamma_2} f(z)dz$$

El lema anterior se deduce del hecho de que si en $\int_{\gamma_1} f(z)dz$ se hace el cambio de variable $z = z' + a$, entonces la curva γ_1 será transformada en la curva γ_2, de lo cual tendremos:

$$\int_{\gamma_1} f(z)dz = \int_{\gamma_2} f(z'+a)dz' = \int_{\gamma_2} f(z')dz' = \int_{\gamma_2} f(z)dz$$

Con estos resultados terminamos nuestro repaso por el cálculo de residuos y variable compleja. Antes de ver algunos lemas, veamos la siguiente definición.

DEFINICIÓN 3.3.22 Sea L una latiz. Un *paralelogramo fundamental (o región fundamental) de la latiz L* es un conjunto de la forma:

$$D = \{a + t_1 w_1 + t w_2 |\ 0 \leqslant t_1,\ t_2 < 1\}$$

en donde $a \in \mathbb{C}$ y w_1, w_2 son los generadores de la latiz L.

LEMA 3.3.23 Sea L una latiz en $\mathbb{C}$. Tomemos una función analítica f en $\mathbb{C}$ que cumpla que $f(z) = f(z+w)$ para cada $z \in \mathbb{C} - L$ y $w \in L$. Si a_k son los ceros y b_j los polos de f dentro de una región fundamental D, en donde la frontera de D (∂D) no pasa por ninguno de los polos o ceros de f entonces:

$$\text{a)} \qquad \sum_k ord(a_k) - \sum_j ord(b_j) = 0$$

$$\text{b)} \qquad \sum_k n(\partial D, a_k)a_k - \sum_j n(\partial D, b_j)b_j \in L$$

DEMOSTRACIÓN. Tomemos una región fundamental D de la latiz L como en la definición 3.3.22. Por el principio del argumento (teorema 3.3.19) sabemos que

$$\frac{1}{2\pi\imath}\int_{\partial D}\frac{f'(z)}{f(z)}dz = \sum_k n(\partial D, a_k) - \sum_j n(\partial D, b_j)$$

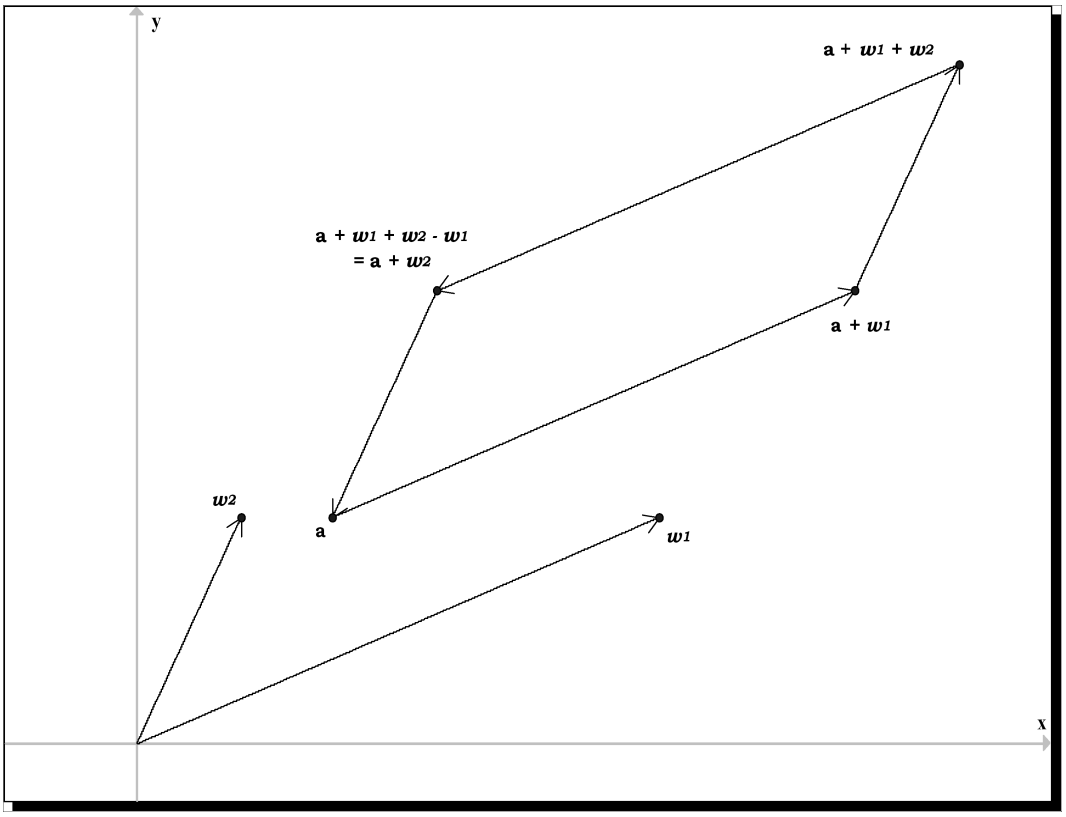
Pero como D es un paralelogramo podemos definir su frontera como la unión de cuatro segmentos dirigidos. Definiremos estos segmentos de la siguiente manera

$$\begin{aligned}
\gamma_1 &= \{z | z = a + tw_1 \quad 0 \leqslant t \leqslant 1\} \\
\gamma_2 &= \{z | z = a + w_1 + tw_2 \quad 0 \leqslant t \leqslant 1\} \\
\gamma_3 &= \{z | z = a + w_1 + w_2 - tw_1 \quad 0 \leqslant t \leqslant 1\} \\
\gamma_4 &= \{z | z = a + w_2 - tw_2 \quad 0 \leqslant t \leqslant 1\}
\end{aligned}$$

con ecuaciones $z_1(t)$, $z_2(t)$, $z_3(t)$ y $z_4(t)$, las cuales describen a la curva respectiva.

Podemos notar que $z_3(t) = z_1(1-t)+w_2$ y $z_2(t) = z_4(1-t)+w_1$, es decir γ_3 es una translación de γ_1 pero se recorren en sentido opuesto. Análogamente sucede con γ_2 y γ_4. De lo anterior por el lema 3.3.21

$$\begin{aligned}
\int_{\gamma_1}\frac{f'(z)}{f(z)}dz &= -\int_{\gamma_3}\frac{f'(z)}{f(z)}dz \\
\text{y} \quad \int_{\gamma_2}\frac{f'(z)}{f(z)}dz &= -\int_{\gamma_4}\frac{f'(z)}{f(z)}dz.
\end{aligned}$$



Por lo que

$$\begin{aligned}\frac{1}{2\pi\imath}\int_{\partial D}\frac{f'(z)}{f(z)}dz &= \frac{1}{2\pi\imath}\int_{\gamma_1}\frac{f'(z)}{f(z)}dz+\frac{1}{2\pi\imath}\int_{\gamma_2}\frac{f'(z)}{f(z)}dz+\\ &\quad \frac{1}{2\pi\imath}\int_{\gamma_3}\frac{f'(z)}{f(z)}dz+\frac{1}{2\pi\imath}\int_{\gamma_4}\frac{f'(z)}{f(z)}dz\\ &= 0,\end{aligned}$$

entonces

$$\frac{1}{2\pi\imath}\int_{\partial D}\frac{f'(z)}{f(z)}dz=\sum_k n(\partial D,a_k)-\sum_j n(\partial D,b_j)=0,$$

si tomamos en cuenta el orden de cada cero o polo tendremos que

$$\frac{1}{2\pi\imath}\int_{\partial D}\frac{f'(z)}{f(z)}dz=\sum_k ord(a_k)\ n(\partial D,a_k)-\sum_j ord(b_j)\ n(\partial D,b_j)=0,$$

y como la curva ∂D da solamente una vuelta alrededor de cada polo o cero de f, entonces

$$\sum_k ord(a_k)\, n(\partial D, a_k) - \sum_j ord(b_j)\, n(\partial D, b_j) = \sum_k ord(a_k) - \sum_j ord(b_j) \ = 0,$$

con lo que queda demostrado a). Para demostrar b) por la generalización del principio del argumento (teorema 3.3.20) tenemos que

$$\frac{1}{2\pi\imath}\int_{\partial D} z\frac{f'(z)}{f(z)} = \sum_k n(\gamma, a_k)a_k - \sum_j n(\gamma, b_j)b_j.$$

Si tomamos la frontera de D como en la demostración de a) tenemos

$$\begin{aligned}\frac{1}{2\pi\imath}\int_{\partial D} z\frac{f'(z)}{f(z)}dz &= \frac{1}{2\pi\imath}\int_{\gamma_1} z\frac{f'(z)}{f(z)}dz + \frac{1}{2\pi\imath}\int_{\gamma_2} z\frac{f'(z)}{f(z)}dz + \\ &\quad + \frac{1}{2\pi\imath}\int_{\gamma_3} z\frac{f'(z)}{f(z)}dz + \frac{1}{2\pi\imath}\int_{\gamma_4} z\frac{f'(z)}{f(z)}dz.\end{aligned}$$

Por la forma en que definimos γ_i (con $i = 1,\ 2,\ 3,\ 4$), podemos hacer el cambio de variable $z = z_i(t)$, por lo que cuando $i = 2$

$$\frac{1}{2\pi\imath}\int_{\gamma_2} z\frac{f'(z)}{f(z)}dz = \frac{1}{2\pi\imath}\int_0^1 z_2(t)\frac{f'(z_2(t))}{f(z_2(t))}z_2'(t)dt.$$

Pero como ya vimos $z_2(t) = z_4(1-t) + w_1$, de tal forma que al hacer este cambio de variable tenemos que $z_2'(t) = -z_4'(1-t)dt$, por lo que

$$\begin{aligned}\frac{1}{2\pi\imath}\int_{\gamma_2} z\frac{f'(z)}{f(z)}dz &= \frac{1}{2\pi\imath}\int_0^1 z_2(t)\frac{f'(z_2(t))}{f(z_2(t))}z_2'(t)dt \\ &= -\frac{1}{2\pi\imath}\int_0^1 \Big(z_4(1-t)+w_1\Big)\frac{f'\big(z_4(1-t)+w_1\big)}{f\big(z_4(1-t)+w_1\big)}z_4'(1-t)dt\end{aligned}$$

Además como $f(z) = f(z+w)$, entonces $f'(z) = f'(z+w)$, por lo que $f'(z)/f(z) = f'(z+w)/f(z+w)$. Así

$$\begin{aligned}\frac{1}{2\pi\imath}\int_{\gamma_2} z\frac{f'(z)}{f(z)}dz &= -\frac{1}{2\pi\imath}\int_0^1 \Big(z_4(1-t)+w_1\Big)\frac{f'\big(z_4(1-t)+w_1\big)}{f\big(z_4(1-t)+w_1\big)}z_4'(1-t)dt \\ &= -\frac{1}{2\pi\imath}\int_0^1 \Big(z_4(1-t)+w_1\Big)\frac{f'\big(z_4(1-t)\big)}{f\big(z_4(1-t)\big)}z_4'(1-t)dt\end{aligned}$$

De aquí si hacemos el cambio de variable $1-t$ por t tenemos

$$\begin{aligned}\frac{1}{2\pi\imath}\int_{\gamma_2} z\frac{f'(z)}{f(z)}dz &= -\frac{1}{2\pi\imath}\int_0^1 \Big(z_4(1-t)+w_1\Big)\frac{f'\big(z_4(1-t)\big)}{f\big(z_4(1-t)\big)}z_4'(1-t)dt\\ &= \frac{1}{2\pi\imath}\int_1^0 \Big(z_4(t)+w_1\Big)\frac{f'\big(z_4(t)\big)}{f\big(z_4(t)\big)}z_4'(t)dt\\ &= -\frac{1}{2\pi\imath}\int_0^1 \Big(z_4(t)+w_1\Big)\frac{f'\big(z_4(t)\big)}{f\big(z_4(t)\big)}z_4'(t)dt\\ &= -\frac{1}{2\pi\imath}\int_{\gamma_4} \Big(z+w_1\Big)\frac{f'\big(z\big)}{f\big(z\big)}dz\end{aligned}$$

de manera análoga, si hacemos algo parecido en la integral alrededor de γ_3 haciendo el cambio de curva a γ_1 tendremos

$$\frac{1}{2\pi\imath}\int_{\gamma_3} z\frac{f'(z)}{f(z)}dz = -\frac{1}{2\pi\imath}\int_{\gamma_1} \Big(z+w_2\Big)\frac{f'\big(z\big)}{f\big(z\big)}dz$$

por las dos últimas ecuaciones tendremos que

$$\begin{aligned}\frac{1}{2\pi\imath}\int_{\partial D} z\frac{f'(z)}{f(z)}dz &= \frac{1}{2\pi\imath}\int_{\gamma_1} z\frac{f'(z)}{f(z)}dz+\frac{1}{2\pi\imath}\int_{\gamma_2} z\frac{f'(z)}{f(z)}dz+\\ &\quad+\frac{1}{2\pi\imath}\int_{\gamma_3} z\frac{f'(z)}{f(z)}dz+\frac{1}{2\pi\imath}\int_{\gamma_4} z\frac{f'(z)}{f(z)}dz\\ &= \frac{1}{2\pi\imath}\int_{\gamma_1} z\frac{f'(z)}{f(z)}dz-\frac{1}{2\pi\imath}\int_{\gamma_4} (z+w_1)\frac{f'(z)}{f(z)}dz\\ &\quad-\frac{1}{2\pi\imath}\int_{\gamma_1} (z+w_2)\frac{f'(z)}{f(z)}dz+\frac{1}{2\pi\imath}\int_{\gamma_4} z\frac{f'(z)}{f(z)}dz\end{aligned}$$

de donde simplificando

$$\frac{1}{2\pi\imath}\int_{\partial D} z\frac{f'(z)}{f(z)}dz = -\frac{w_2}{2\pi\imath}\int_{\gamma_1}\frac{f'(z)}{f(z)}dz-\frac{w_1}{2\pi\imath}\int_{\gamma_4}\frac{f'(z)}{f(z)}dz$$

Ahora bien, si hacemos el cambio de variable $\widetilde{z}=f(z)$, tendremos que $d\widetilde{z}=f'(z)dz$. Con este cambio de variable la curva γ_1 se convertirá en la curva

$$\overline{\gamma_1}=\{\widetilde{z}\mid \widetilde{z}=f(z),\quad \text{en donde } z\in\gamma_1\}$$

con esto tenemos

$$\frac{w_2}{2\pi\imath}\int_{\gamma_1}\frac{f'(z)}{f(z)}dz \;=\; \frac{w_2}{2\pi\imath}\int_{\overline{\gamma_1}}\frac{d\widetilde{z}}{\widetilde{z}}$$

Debemos notar que como en la curva $\overline{\gamma_1}$, $f(a) = f(b)$, entonces $\overline{\gamma_1}$ es cerrada, por lo que podemos ocupar el principio del argumento (Teorema 3.3.19), de lo cual

$$\frac{1}{2\pi\imath}\int_{\gamma_1}\frac{f'(z)}{f(z)}dz = \frac{1}{2\pi\imath}\int_{\overline{\gamma_1}}\frac{d\widetilde{z}}{\widetilde{z}} = n(\overline{\gamma_1},0)\in\mathbb{Z}$$

ya que esta integral nos arrojará como resultado la suma del número de giros que da la curva alrededor de cada cero de la función $\widetilde{z}$ menos la suma del número de giros que da la curva alrededor de cada polo de la función $\widetilde{z}$ dentro de la curva. Por lo que existe $m\in\mathbb{Z}$ tal que

$$\frac{w_2}{2\pi\imath}\int_{\gamma_1}\frac{f'(z)}{f(z)}dz = mw_2$$

De manera análoga podemos ver que existe $n\in\mathbb{Z}$ tal que

$$\frac{w_1}{2\pi\imath}\int_{\gamma_4}\frac{f'(z)}{f(z)}dz = nw_1$$

de lo anterior deducimos que

$$\begin{aligned}\frac{1}{2\pi\imath}\int_{\partial D} z\frac{f'(z)}{f(z)}dz &= \frac{w_2}{2\pi\imath}\int_{\gamma_1}\frac{f'(z)}{f(z)}dz + \frac{w_1}{2\pi\imath}\int_{\gamma_4}\frac{f'(z)}{f(z)}dz\\ &= mw_2+nw_1\in L\end{aligned}$$

y como ya habíamos visto al principio de la demostracíon que

$$\frac{1}{2\pi\imath}\int_{\partial D} z\frac{f'(z)}{f(z)} = \sum_k n(\gamma,a_k)a_k - \sum_j n(\gamma,b_j)b_j$$

de donde finalmente obtendremos que

$$\sum_k n(\gamma,a_k)a_k - \sum_j n(\gamma,b_j)b_j\in L$$

que es lo que queríamos demostrar. ∎

COROLARIO 3.3.24 Cuando $n(\gamma, a_k)$ y $n(\gamma, b_j)$ es 1, si el orden de cada cero es $ord(a_k)$ y el orden de cada polo es $ord(b_k)$ entonces:

$$\sum_k ord(a_k)a_k - \sum_j ord(b_j)b_j \in L$$

Además de los resultados de variable compleja que ya hemos visto deberemos hacer la siguiente anotación sobre curvas elípticas en un lema.

LEMA 3.3.25 Sea $z \in \mathbb{C}$ tal que $\frac{z}{2} \notin L$. Entonces z está en L si y sólo si $\wp'(z/2) = 0$

DEMOSTRACIÓN.

$\Rightarrow$) Tomemos $w \in L$. Por el lema 3.3.7 tendremos que $\wp'(z) = \wp'(z + w)$ para todo $z \in \mathbb{C} - L$ y toda $w \in L$, entonces como por hipótesis $w/2 \notin L$ (es decir, $w \in \mathbb{C} - L$) tenemos que

$$\wp'(w/2) = \wp'(w/2 - w) = \wp'(-w/2),$$

y por el lema 3.3.7 también sabemos que la función $\wp'$ es impar, entonces

$$\wp'(-w/2) = -\wp'(w/2),$$

así

$$\wp'(w/2) = -\wp'(w/2),$$

por lo que

$$2\wp'(w/2) = \wp'(w/2) + \wp'(w/2) = \wp'(w/2) - \wp'(w/2) = 0,$$

por lo tanto, si $w \in L$, entonces $\wp'(w/2) = 0$.

$\Leftarrow$) Hagamos esto por reducción al absurdo. Para ello supongamos que existe algún $z_1 \notin L$ tal que $\wp'(z_1/2) = 0$. Tomemos w_1 y w_2 como los generadores de la latiz L. Además tomemos una región fundamental D que contenga a $w_1/2$, $w_2/2$ y $(w_1+w_2)/2$, y busquemos un punto z_2 tal que $z_2 \in D$ y que $z_2 \equiv z_1 \pmod{L}$. Dentro de esta región analizaremos qué pasa con la función ϕ_1, la cual definiremos como $\phi_1(z) = \wp(z) - \wp(w_1/2)$. En esta región D habrá solamente un

punto de la latiz L, al cual llamaremos w_a. Debemos notar que nos basta con analizar ϕ en D ya que por el lema 3.3.7 $\wp(z) = \wp(z+w)$ y $\wp'(z) = \wp'(z+w)$ para toda $z \in \mathbb{C} - L$ y toda $w \in L$, por lo que analizando lo que pasa con ϕ en D sabremos lo que pasa con ϕ en $\mathbb{C}$.

Como los puntos w_1, w_2 y w_1+w_2 pertenecen a L entonces tendremos por la demostración de la implicación ($\Rightarrow$) que $\wp'(w_1/2)$, $\wp'(w_2/2)$ y $\wp'\Big((w_1+w_2)/2\Big)$ son 0. Por otro lado la función ϕ_1 tiene un cero en $w_1/2$, pero como $\wp'(w_1/2) = 0$, entonces ϕ_1 tiene un cero de orden al menos 2 en $w_1/2$. Además en el teorema 3.3.8 vimos que la función $\wp(z)$ tiene un polo de orden 2 en cada punto de L y ya que la función $\wp(w_1/2)$ es una constante no tiene polos, por lo que la función $\phi_1(z)$ tendrá un polo de orden 2 en cada punto de L.

De tal manera que en la región fundamental D tenemos en w_a un polo de orden 2 de ϕ_1 (el cual es el único) y en $w_1/2$ un cero de orden al menos 2 también de ϕ_1. Del lema 3.3.23 tenemos que la suma de los órdenes de los ceros menos la suma de los órdenes de los polos es 0. Como para la función ϕ_1 dentro de la región D, con el cero y el polo que tenemos, la diferencia de los órdenes es 0 y ya que el polo es único en D, entonces podemos descartar que exista algún otro cero de la función ϕ_1 en la región D (porque de haberlo sería de orden al menos 1, que más el orden de w_1 obtendríamos como suma de los órdenes de los ceros 3, lo cual es diferente del orden del polo).

Con esto concluimos que $\phi_1(z)$ solamente tiene un cero en $w_1/2$, dentro de D y que además este cero es de orden exactamente 2, lo cual quiere decir que $\phi_1(z) \neq 0$ para toda z distinta de $w_1/2$, es decir, $\wp(z) - \wp(w_1/2) \neq 0$. En particular, ϕ_1 es distinta de cero en $w_2/2$, $(w_1+w_2)/2$ y $z_2/2$ ($z_2/2 \neq w_1/2$, pues de lo contrario $z_1 \in L$), lo cual quiere decir que

$$\begin{aligned} \wp(w_1/2) &\neq \wp(w_2/2) \\ \wp(w_1/2) &\neq \wp\big((w_1+w_2)/2\big) \\ \wp(w_1/2) &\neq \wp(z_2/2) \end{aligned}$$

De manera análoga podemos tomar $\phi_2(z) = \wp(z) - \wp(w_2/2)$ y $\phi_3(z) = \wp(z) - \wp\big((w_1+w_2)/2\big)$, en las cuales podemos encontrar que $\phi_2(z)$

solamente tiene ceros en $w_2/2$ y $\phi_3(z)$ sólo tiene ceros en $(w_1+w_2)/2$ dentro de D, de lo cual podemos concluir que

$$\begin{aligned}
\wp(w_2/2) &\neq \wp(w_1/2)\\
\wp(w_2/2) &\neq \wp\big((w_1+w_2)/2\big)\\
\wp(w_2/2) &\neq \wp(z_2/2)\\
\wp\big((w_1+w_2)/2\big) &\neq \wp(w_1/2)\\
\wp\big((w_1+w_2)/2\big) &\neq \wp(w_2/2)\\
\wp\big((w_1+w_2)/2\big) &\neq \wp(z_2/2)
\end{aligned}$$

Por lo que

$$\begin{aligned}
\wp(w_1/2) &\neq \wp(w_2/2)\\
\wp(w_1/2) &\neq \wp\big((w_1+w_2)/2\big)\\
\wp(w_1/2) &\neq \wp(z_2/2)\\
\wp(w_2/2) &\neq \wp\big((w_1+w_2)/2\big)\\
\wp(w_2/2) &\neq \wp(z_2/2)\\
\wp(z_2/2) &\neq \wp\big((w_1+w_2)/2\big)
\end{aligned}$$

En este punto sería bueno preguntarnos ¿esto de que nos va a servir? Pues bien tomemos la curva elíptica que construimos para la región D. La ecuación de esta curva elíptica es de la forma $\Big(\wp'(z)\Big)^2 = 4\wp(z)^3 - 60G_4\wp(z) + 140G_6$. Tanto en $w_1/2$, $w_2/2$, $(w_1+w_2)/2$ como en $z_2/2$ la función $\wp'(z)$ es 0, por lo que si tomamos la función $f(x) = 4x^3 - 60G_4x + 140G_6$ entonces $\wp(w_1/2)$, $\wp(w_2/2)$, $\wp\big((w_1+w_2)/2\big)$ y $\wp(z_2/2)$ son raíces de $f(x)$. Pero como vimos cada uno de estos puntos es distinto de los demás, por lo que tenemos 4 raíces distintas de f, pero al ser f un polinomio de grado 3 solamente puede tener 3 raíces y tenemos cuatro lo cual es una contradicción.

Con esto demostramos que nuestras suposiciones fueron incorrectas por lo que podemos concluir que, si $\wp'(z/2) = 0$, entonces $z \in L$. Con esto concluimos la demostración

■

Con este último resultado podremos dar paso a la demostración de la propiedad 3, recordemos primero qué es lo que dice:

Propiedad 3) Dos números complejos z_1 y $z_2 \in \mathbb{C} - L$ dan el mismo punto $(\wp(z), \wp'(z))$ en $\mathbf{E}$ si y sólo si $z_1 - z_2 \in L$.

Para demostrar la parte del "si" tomemos $z_1 - z_2 \in L$. Entonces existe alguna $w \in L$ tal que $z_1 - z_2 = w$, es decir, $z_1 = w + z_2$ y por el lema 3.3.7 tenemos que

$$\wp(z_1) = \wp(z_2 + w) = \wp(z_2) \quad \text{y}$$
$$\wp'(z_1) = \wp'(z_2 + w) = \wp'(z_2).$$

Por tanto los puntos $(\wp(z_1), \wp'(z_1))$ y $(\wp(z_2), \wp'(z_2))$ coinciden. Nos falta demostrar la parte del "sólo si". Para probarla comenzaremos tomando dos puntos z_1 y z_2 en $\mathbb{C}$ y supongamos que $\wp(z_1) = \wp(z_2)$ y $\wp'(z_1) = \wp'(z_2)$. Construyamos la función $\phi(z) = \wp(z) - \wp(z_1)$. Continuamos la demostración tomando dos casos, cuando $2z_1 \in L$ y cuando $2z_1 \notin L$.

Caso 1) $2z_1 \notin L$

Si $2z_1 \notin L$, entonces $z_1 + z_1 \notin L$. Así que ni $2z_1$ ni z_1 pertenecen a L. Podemos aplicar el lema 3.3.25 obteniendo que $\wp'(z_1) \neq 0$. Como $-\wp(z_1)$ es una constante y $\wp(z)$ tiene un polo de orden 2 en cada punto de L, entonces $\phi(z)$ tiene un polo de orden 2 en cada punto de L. Además por el lema 3.3.7, como $\wp$ es par tenemos que $\wp(z_1) = \wp(-z_1)$. Como $\wp(z_1) = \wp(z_2)$, los números z_1, $-z_1$ y z_2 son ceros de $\phi(z)$.

Tomemos una región fundamental D_1 tal que $z_1 \in D_1$ pero que la frontera de D_1 (∂D_1) no pase por ninguno de los ceros o polos de ϕ. En esta región tomemos un punto z_3 tal que $z_3 \equiv z_2 \pmod{L}$.

Tomemos como γ a ∂D_1 en el corolario 3.3.24 con la función $\phi(z)$. Como D_1 contiene a un polo w de orden 2 ($w \in L$), D_1 sólo puede tener un cero de orden 2 o dos ceros de orden 1, para que se cumpla la fórmula de dicho corolario. Notemos que z_1, $z_3 \in D_1$ y que ambos son ceros de $\phi(z)$. De manera que $z_1 = z_3$ o z_1 y z_3 son ceros de orden 1. En el primer caso tenemos que $z_1 \equiv z_2 \pmod{L}$ y ya acabamos, en el segundo caso, la fórmula del corolario 3.3.24 nos dice que $z_1 + z_3 + 2w \in L$. Así que $z_1 + z_3 \in L$ y $z_3 \equiv -z_1 \pmod{L}$. Por tanto $z_2 \equiv -z_1 \pmod{L}$.

Sabemos por hipótesis que $\wp'(z_1) = \wp'(z_2)$. Por la parte del "si" de esta demostración tenemos que $\wp'(z_2) = \wp'(-z_1)$, como $\wp'$ es impar, $\wp'(z_2) = \wp'(-z_1) = -\wp'(z_1)$. Por hipótesis $\wp'(z_2) = \wp'(z_1)$, entonces $\wp'(z_1) = -\wp'(z_1)$. Así que $2\wp'(z_1) = \wp'(z_1) + \wp'(z_1) = \wp'(z_1) - \wp'(z_1) = 0$, de donde, $\wp'(z_1) = 0$. Esto contradice el hecho de que $\wp'(z_1) \neq 0$, por lo que no puede ocurrir que $z_2 \equiv -z_1 \pmod{L}$, por lo que necesariamente $z_2 \equiv z_1 \pmod{L}$.

Caso 2) $2z_1 \in L$

Como $\wp(z_1) = \wp(z_2)$ y $\wp'(z_1) = \wp'(z_2)$, $\phi(z_2) = 0$. Como $2z_1 \in L$, por el lema 3.3.25, $\wp'(z_1) = 0$. Notemos que $\phi(z_1) = 0$, entonces $\phi(z)$ tiene un cero de orden al menos 2 en z_1. Si construimos una región D_1 como en el caso 1) y tomamos un punto z_3 tal que $z_3 \equiv z_2 \pmod{L}$, entonces $\phi(z_3) = 0$ (ya que $\phi(z_2) = 0$). Por el lema 3.3.23, dado que z_3 es un cero de ϕ, z_1 es un cero de orden al menos 2 y existe un punto $w \in D_1$ que es un polo de orden 2, concluimos que $z_1 = z_3$ por lo que $z_2 \equiv z_1 \pmod{L}$.

De ambos casos concluimos que, si $\wp(z_1) = \wp(z_2)$ y $\wp'(z_1) = \wp'(z_2)$, entonces $z_2 \equiv z_1 \pmod{L}$ con lo cual completamos la demostración de la propiedad 3.

Ahora recordemos la propiedad 4, y a continuación demos su demostración.

Propiedad 4) La función que le asocia a un punto $z \notin L$ el correspondiente punto $(\wp(z), \wp'(z))$ en $\mathbf{E}$ y le asocia a los puntos $z \in L$ el punto al infinito $O \in \mathbf{E}$ da una correspondencia uno a uno entre $\mathbf{E}$ y el cociente del plano complejo por el subgrupo L (denotado $\mathbb{C}/L$).

Para demostrar la propiedad 4 denotemos por $\phi(z)$ a la función entre el cociente del plano complejo por el subgrupo L (denotado $\mathbb{C}/L$) y $\mathbf{E}$, es decir,

$$\phi \ : \ \mathbb{C}/L \to \mathbf{E}$$

Dada por

$$\phi(z) = \begin{cases} (\wp(z), \wp'(z)), & \text{si } z \notin L \\ O, & \text{si } z \in L \end{cases}$$

Lo primero que tendríamos que demostrar es que ϕ está bien definida, es decir, que para cualesquiera z' y z'' en la clase $z + L$ en $\mathbb{C}/L$ tenedremos que $\phi(z') = \phi(z'')$. Pero Si z' y z'' están en $z + L$ entonces existe $w \in L$

tal que $z' = w + z''$, por lo que $\wp(z') = \wp(z'')$ y $\wp'(z') = \wp'(z'')$, por lo que $\phi(z') = \phi(z'')$. Ahora demostraremos que la función ϕ es biyectiva. Para demostrar que es inyectiva primero notemos que si $z_1 \in L$ y $z_2 \notin L$, entonces $\phi(z_1) = O$ y $\phi(z_2) \neq O$, así que $\phi(z_1) \neq \phi(z_2)$. Ahora si z_1, $z_2 \in \mathbb{C} - L$ y

$$(\wp(z_1), \wp'(z_1)) = (\wp(z_2), \wp'(z_2)),$$

entonces por la propiedad 3, $z_1 \equiv z_2 \pmod{L}$. Por tanto ϕ es inyectiva.

Para demostrar que ϕ es suprayectiva tomemos una pareja $(x, y) \in \mathbf{E} - \{O\}$. Construyamos la función $g(z) = \wp(z) - x$ la cual no es una función constante (una función con polos no puede ser constante), notemos que también tiene al menos un cero[6], digamos que este cero es $z = a$, entonces $\wp(a) = x$. Por la fórmula que define a $\mathbf{E}$ (ver teorema 3.3.11),

$$\begin{aligned}(\wp'(a))^2 &= 4(\wp(a))^3 - 60G_4\wp(a) - 140G_6 \\ &= 4x^3 - 60G_4x - 140G_6 \\ &= y^2,\end{aligned}$$

(notemos que $a \notin L$ porque en el punto a $\wp$ está definida). De manera que $(\wp'(a))^2 = y^2$. Así que $y = \wp'(a)$ o $y = -\wp'(a)$. En el caso en que $y = \wp'(a)$, tenemos que $\phi(a) = (x, y)$. Y en el caso en que $y = -\wp'(a)$, como $\wp'$ es impar (por el lema 3.3.7), entonces $(x, y) = (\wp(a), -\wp'(a)) = (\wp(-a), \wp'(-a))$. Por tanto $\phi(-a) = (x, y)$. Por tanto ϕ es suprayectiva.

Por último debemos demostrar la propiedad 5 la cual dice:

La función ϕ es un isomorfismo de grupos abelianos.

En otras palabras, si a $z_1 \in \mathbb{C}$ le corresponde el punto $P \in \mathbf{E}$ y a $z_2 \in \mathbb{C}$ le corresponde el punto $Q \in \mathbf{E}$, entonces al número complejo $z_1 + z_2$ corresponde el punto $P + Q$. Es decir $\phi(z_1) + \phi(z_2) = \phi(z_2 + z_1)$.

Dado que $\phi(z) = (\wp(z), \wp'(z))$, debemos demostrar que

$$\begin{aligned}\wp(z_1) + \wp(z_2) &= \wp(z_1 + z_2) \quad \text{y} \\ \wp'(z_1) + \wp'(z_2) &= \wp'(z_1 + z_2).\end{aligned}$$

[6] La función g satisface las condiciones del teores 3.3.23, por lo que, si g no tiene ceros, entonces tampoco tiene polos, pero los polos de $\wp$ también lo son de g. El argumento anterior nos llevaría a una contradicción por lo que g tiene al menos un cero.

Analicemos primero el caso cuando alguno de los puntos (digamos z_1) está en L y el otro punto (z_2) está en $\mathbb{C} - L$. En este caso $\phi(z_1) = O$, entonces

$$\phi(z_1 + z_2) = (\wp(z_1 + z_2), \wp'(z_1 + z_2))$$

al estar $z_1 \in L$, entonces

$$\begin{aligned} \phi(z_1 + z_2) &= (\wp(z_1 + z_2), \wp'(z_1 + z_2)) \\ &= (\wp(z_2), \wp'(z_2)) \\ &= \phi(z_2) = \phi(z_2) + O \\ &= \phi(z_2) + \phi(z_1). \end{aligned}$$

Cuando z_1 y $z_2 \in L$, también $z_1 + z_2 \in L$, por lo que

$$\phi(z_1 + z_2) = \phi(z_1) + \phi(z_2).$$

Finalmente veamos el caso en que tanto z_1 como z_2 no están en L. Para ver esto debemos recordar que en el lema 3.2.1 vimos que dados dos puntos en una curva elíptica, digamos (x_1, y_1) y (x_2, y_2), las coordenadas del punto que es la suma de estos dos puntos están dadas por:[7]

$$\begin{aligned} x_3 &= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \\ y_3 &= -y_1 + (x_1 - x_3)\left(\frac{y_2 - y_1}{x_2 - x_1}\right), \end{aligned}$$

[7] Recordemos que x_3 se obtiene de despejar esta variable de la ecuación $m^2 = x_1 + x_2 + x_3$, en donde m es la ecuación de la pendiente de la recta que pasa por (x_1, y_1) y (x_2, y_2), y $x_1 + x_2 + x_3$ es menos el coeficiente del término cuadratico del polinomio $(x - x_1)(x - x_2)(x - x_3)$ y $-y_3$ se obtiene de sustituir x_3 por x en la ecuación de la recta que pasa por (x_1, y_1) y (x_2, y_2), es decir, en $-y_3 = m(x_3 - x_1) + y_1$.

esto en el caso en que la ecuación de la curva fuera de la forma $y^2 = x^3+dx+e$. Tomando en cuenta que la ecuación que tenemos de la curva elíptica es de la forma $y^2 = 4x^3 + dx + e$, entonces las ecuaciones para x_3 y y_3 quedan en la forma[8]

$$\begin{aligned} x_3 &= \frac{1}{4}\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \\ y_3 &= -y_1 + (x_1 - x_3)\left(\frac{y_2 - y_1}{x_2 - x_1}\right). \end{aligned}$$

Entonces necesitamos demostrar que

$$\begin{aligned} \wp(z_1 + z_2) &= \frac{1}{4}\left(\frac{\wp'(z_2) - \wp'(z_1)}{\wp(z_2) - \wp(z_1)}\right)^2 - \wp(z_1) - \wp(z_2) \\ \wp'(z_1 + z_2) &= -\wp'(z_1) + \big(\wp(z_1) - \wp(z_1 + z_2)\big)\left(\frac{\wp'(z_2) - \wp'(z_1)}{\wp(z_2) - \wp(z_1)}\right). \end{aligned}$$

Si demostramos la igualdad de $\wp(z_1 + z_2)$ se puede seguir la demostración que se dio para encontrar y_3 a partir de x_3 y con ello encontrar $\wp'(z_1 + z_2)$ a partir de $\wp(z_1 + z_2)$. Para encontrar el valor de $\wp(z_1 + z_2)$ necesitaremos ver algunas ecuaciones primero.

Como vimos en la página 86, el desarrollo en serie de Laurent de la función $\wp(z)$ tiene coeficiente 0 en el término $\frac{1}{z-w_0}$, por lo que $\wp(z)$ deberá ser la derivada de una función univaluada (esto ya que cada término de la serie de Laurent de $\wp$ es integrable). Como $\wp$ está definida por

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{w \in L \\ w \neq 0}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2}\right),$$

[8] De acuerdo a la nota anterior la ecuación de m no cabiaría. Al ser la ecuación de la curva $y^2 = 4x^3 + dx + e$, entonces nos fijaremos ahora en menos el término cuadratico del porinomio $4(x-x_1)(x-x_2)(x-x_3)$ y este lo igualaremos a m^2, es decir, $m^2 = 4(x_1+x_2+x_3)$, del que despejaremos x_3, por lo que

$$x_3 = \frac{m^2}{4} - x_2 - x_3$$

con lo que y_3 estará dada por

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

podemos definir una función $\zeta(z)$ por:

$$\zeta(z) = \frac{1}{z} + \sum_{\substack{w \in L \\ w \neq 0}} \left(\frac{1}{z-w} + \frac{1}{w} + \frac{z}{w^2} \right),$$

de tal manera que

$$\wp(z) = -\zeta'(z).$$

Otra función que utilizaremos es:

$$\sigma(z) = z \prod_{\substack{w \in L \\ w \neq 0}} \left(1 - \frac{z}{w}\right) e^{z/w + \frac{1}{2}(z/w)^2},$$

se puede demostrar que esta función converge[9], además de que satisface

$$\frac{\sigma'(z)}{\sigma(z)} = \zeta(z),$$

es decir

$$\frac{d}{dz} log\big(\sigma(z)\big) = \zeta(z),$$

Aplicando la definición de σ se tiene que:

$$\begin{aligned}
&\frac{\sigma(z+a)\sigma(z-a)}{\big(\sigma(z)\big)^2} \\
&= \frac{(z+a)(z-a)\prod_{\substack{w \in L \\ w \neq 0}} \big(1 - \frac{z+a}{w}\big)\big(1 - \frac{z-a}{w}\big) e^{\frac{z+a}{w} + \frac{1}{2}\left(\frac{z+a}{w}\right)^2 + \frac{z-a}{w} + \frac{1}{2}\left(\frac{z-a}{w}\right)^2}}{z^2 \prod_{\substack{w \in L \\ w \neq 0}} \left(1 - \frac{z}{w}\right)^2 e^{2\frac{z}{w} + \frac{z^2}{w^2}}} \\
&= \frac{(z^2-a^2)\prod_{\substack{w \in L \\ w \neq 0}} \big(\frac{(w-z)^2 - a^2}{w^2}\big) e^{2\frac{z}{w} + \frac{z^2+a^2}{w}}}{z^2 \prod_{\substack{w \in L \\ w \neq 0}} \left(\frac{w-z}{w}\right)^2 e^{2\frac{z}{w} + \frac{z^2}{w^2}}} \\
&= \frac{(z^2-a^2)}{z^2} \prod_{\substack{w \in L \\ w \neq 0}} \left(\frac{(w-z)^2 - a^2}{(w-z)^2}\right) e^{a^2/w^2}
\end{aligned}$$

[9] página 274 de [**?**]

Si definimos $h(z)$ para $a \notin L$, como

$$h(z) = \frac{\sigma(z+a)\sigma(z-a)}{\big(\sigma(z)\big)^2},$$

y sustituimos z por $w_0 + a$, donde $w_0 \in L$ obtenemos

$$\begin{aligned}
h(w_0+a) &= \frac{((w_0+a)^2-a^2)}{(w_0+a)^2} \prod_{\substack{w\in L\\ w\neq 0}} \left(\frac{(w-(w_0+a))^2-a^2}{(w-(w_0+a))^2}\right) e^{a^2/w^2} \\
&= \frac{((w_0+a)^2-a^2)}{(w_0+a)^2} \left(\frac{(w_0-(w_0+a))^2-a^2}{(w_0-(w_0+a))^2}\right) e^{a^2/(w_0)^2} \times \\
&\quad \times \prod_{\substack{w\in L\\ w\neq 0\\ w\neq w_0}} \left(\frac{(w-(w_0+a))^2-a^2}{(w-(w_0+a))^2}\right) e^{a^2/w^2} \\
&= \frac{((w_0+a)^2-a^2)}{(w_0+a)^2} \left(\frac{a^2-a^2}{a^2}\right) e^{a^2/(w_0)^2} \times \\
&\quad \times \prod_{\substack{w\in L\\ w\neq 0\\ w\neq w_0}} \left(\frac{(w-(w_0+a))^2-a^2}{(w-(w_0+a))^2}\right) e^{a^2/w^2} \\
&= \frac{((w_0+a)^2-a^2)}{(w_0+a)^2} \left(\frac{0}{a^2}\right) e^{a^2/(w_0)^2} \times \\
&\quad \times \prod_{\substack{w\in L\\ w\neq 0\\ w\neq w_0}} \left(\frac{(w-(w_0+a))^2-a^2}{(w-(w_0+a))^2}\right) e^{a^2/w^2} \\
&= 0,
\end{aligned}$$

por lo que $h(z)$ tiene ceros en $a+w$ para toda $w \in L$ y polos en cada punto $w \in L$ (pues $\sigma(w+a) \neq 0$ y $\sigma(w-a) \neq 0$ para toda $w \in L$), al igual que la función $\wp(z) - \wp(a)$ (semejante a lo que se hizo con ϕ_1 en la demostración de $\Leftarrow$ del lema 3.3.25), por lo que $h(z)$ y $\wp(z) + \wp(a)$ son iguales o una es un múltiplo de la otra, es decir,

$$\wp(z) - \wp(a) = C\ h(z) = C\left(\frac{\sigma(z+a)\sigma(z-a)}{\big(\sigma(z)\big)^2}\right),$$

para alguna constante C. Si multiplicamos ambos lados de la igualdad ante-

rior por z^2 obtenemos:

$$z^2\wp(z) - z^2\wp(a) = Cz^2\left(\frac{\sigma(z+a)\sigma(z-a)}{\big(\sigma(z)\big)^2}\right),$$

pero recordando que

$$z^2\wp(z) = \frac{z^2}{z^2} + \sum_{\substack{w\in L\\ w\neq 0}}\left(\frac{z^2}{(w-z)^2} - \frac{z^2}{w^2}\right),$$

cuando hacemos tender z hacia 0 en $z^2\wp(z)$ tendremos:

$$\begin{aligned} z^2\wp(z) &= \frac{z^2}{z^2} + \sum_{\substack{w\in L\\ w\neq 0}}\left(\frac{z^2}{(w-z)^2} - \frac{z^2}{w^2}\right) \\ &\to 1 + \sum_{\substack{w\in L\\ w\neq 0}}(0-0) = 1. \end{aligned}$$

Además como $\wp(a)$ es una constante, $z^2\wp(a) \to 0$ cuando $z \to 0$. Por otro lado cuando hacemos tender z hacia 0 en la función $z^2/(\sigma(z))^2$ obtenemos

$$\begin{aligned} \frac{z^2}{(\sigma(z))^2} &= \frac{z^2}{z^2\prod_{\substack{w\in L\\ w\neq 0}}\left(1-\frac{z}{w}\right)^2 e^{2z/w+(z/w)^2}} = \frac{1}{\prod_{\substack{w\in L\\ w\neq 0}}\left(1-\frac{z}{w}\right)^2 e^{2z/w+(z/w)^2}} \\ &\to \frac{1}{1\prod_{\substack{w\in L\\ w\neq 0}}\left(1-0\right)^2 e^{0+(0)^2}} = \frac{1}{1\prod_{\substack{w\in L\\ w\neq 0}}(1)^2 e^0} = 1. \end{aligned}$$

También podemos notar que cuando $z \to 0$ entonces $\sigma(z+a)\sigma(z-a) \to \sigma(a)\sigma(-a)$ pero

$$\begin{aligned} \sigma(a) &= a\prod_{\substack{w\in L\\ w\neq 0}}\left(1-\frac{a}{w}\right)e^{a/w+\frac{1}{2}(a/w)^2} \\ &= a\prod_{\substack{w\in L\\ w\neq 0}}\left(1-\frac{(-a)}{(-w)}\right)e^{(-a)/(-w)+\frac{1}{2}\left((-a)/(-w)\right)^2} \\ &= -\left[-a\prod_{\substack{w\in L\\ w\neq 0}}\left(1-\frac{(-a)}{(-w)}\right)e^{(-a)/(-w)+\frac{1}{2}\left((-a)/(-w)\right)^2}\right], \end{aligned}$$

si hacemos el cambio de variable $-w$ por w_0 en la ultima igualdad, los puntos w_0 siguen siendo distintos de 0 y siguen perteneciendo a L, por lo que la última ecuación queda como:

$$\begin{aligned}\sigma(a) &= -\left[-a \prod_{\substack{w\in L\\ w\neq 0}} \left(1-\frac{(-a)}{(-w)}\right) e^{(-a)/(-w)+\frac{1}{2}\left((-a)/(-w)\right)^2}\right] \\ &= -\left[-a \prod_{\substack{w\in L\\ w_0\neq 0}} \left(1-\frac{(-a)}{w_0}\right) e^{(-a)/w_0+\frac{1}{2}\left((-a)/w_0\right)^2}\right] \\ &= -\sigma(-a),\end{aligned}$$

por lo que $\sigma(z+a)\sigma(z-a) \rightarrow \ \sigma(a)\sigma(-a) = -\big(\sigma(a)\big)^2$. De lo anterior tendremos que si juntamos los últimos resultados y los aplicamos a la igualdad

$$z^2\wp(z) - z^2\wp(a) = Cz^2\left(\frac{\sigma(z+a)\sigma(z-a)}{\big(\sigma(z)\big)^2}\right),$$

entonces podemos notar que cuando z tiende a 0

$$\begin{aligned} z^2\wp(z) - z^2\wp(a) &= Cz^2\left(\frac{\sigma(z+a)\sigma(z-a)}{\big(\sigma(z)\big)^2}\right) \\ z^2\wp(z) - z^2\wp(a) &= C\left(\frac{z^2}{\big(\sigma(z)\big)^2}\right)\sigma(z+a)\sigma(z-a) \\ \Rightarrow \ 1-0 &= C(1)\Big(-\big(\sigma(a)\big)^2\Big) \\ \Rightarrow \ 1 &= -C\big(\sigma(a)\big)^2 \\ \Rightarrow \ C &= -\frac{1}{\big(\sigma(a)\big)^2}.\end{aligned}$$

Recordando que teníamos

$$\wp(z) - \wp(a) = C\left(\frac{\sigma(z+a)\sigma(z-a)}{\big(\sigma(z)\big)^2}\right).$$

Al sustituir C obtenemos

$$\wp(z) - \wp(a) = -\frac{\sigma(z+a)\sigma(z-a)}{\big(\sigma(z)\big)^2\big(\sigma(a)\big)^2}.$$

Si aplicamos el logaritmo natural de ambos lados de la última igualdad obtenemos

$$\begin{aligned} log\big(\wp(z)-\wp(a)\big) &= log\Big(-\frac{\sigma(z+a)\sigma(z-a)}{\big(\sigma(z)\big)^2\big(\sigma(a)\big)^2}\Big) \\ &= log\big(\sigma(z+a)\big)+log\big(\sigma(z-a)\big)- \\ &\quad -log\big[\big(\sigma(z)\big)^2\big]-log\big[-\big(\sigma(a)\big)^2\big] \\ &= log\big(\sigma(z+a)\big)+log\big(\sigma(z-a)\big)- \\ &\quad -2log\big(\sigma(z)\big)-log\big[-\big(\sigma(a)\big)^2\big], \end{aligned}$$

derivando ambos lados de esta igualdad obtenemos

$$\begin{aligned} \frac{d}{dz}log\big(\wp(z)-\wp(a)\big) &= \frac{d}{dz}\Big(log\big(\sigma(z+a)\big)+log\big(\sigma(z-a)\big)- \\ &\quad -2log\big(\sigma(z)\big)-log\big[-\big(\sigma(a)\big)^2\big]\Big) \\ \frac{\wp'(z)}{\wp(z)-\wp(a)} &= \frac{\sigma'(z+a)}{\sigma(z+a)}+\frac{\sigma'(z-a)}{\sigma(z-a)}-2\frac{\sigma'(z)}{\sigma(z)}. \end{aligned}$$

Como $\sigma'(z)/\sigma(z)=\zeta(z)$, entonces

$$\begin{aligned} \frac{\wp'(z)}{\wp(z)-\wp(a)} &= \frac{\sigma'(z+a)}{\sigma(z+a)}+\frac{\sigma'(z-a)}{\sigma(z-a)}-2\frac{\sigma'(z)}{\sigma(z)} \\ &= \zeta(z+a)+\zeta(z-a)-2\zeta(z). \end{aligned}$$

Si repetimos lo anterior, pero suponiendo ahora que la variable es a y z una constante obtenemos

$$\frac{-\wp'(a)}{\wp(z)-\wp(a)} = \zeta(z+a)-\zeta(z-a)-2\zeta(a),$$

sumando las dos últimas ecuaciones resulta que

$$\begin{aligned} \frac{\wp'(z)}{\wp(z)-\wp(a)}+\frac{-\wp'(a)}{\wp(z)-\wp(a)} &= \zeta(z+a)+\zeta(z-a)-2\zeta(z)+ \\ &\quad \Big(\zeta(z+a)-\zeta(z-a)-2\zeta(a)\Big), \end{aligned}$$

y

$$\frac{\wp'(z)-\wp'(a)}{\wp(z)-\wp(a)} = 2\zeta(z+a)-2\zeta(z)-2\zeta(a),$$

por lo que

$$\zeta(z+a) = \zeta(z) + \zeta(a) + \frac{1}{2}\frac{\wp'(z) - \wp'(a)}{\wp(z) - \wp(a)}.$$

Si derivamos ambos lados de la última ecuación con respecto a z, ya que $\int \wp(z) = -\zeta(z)$ y $\wp(z) = -\zeta'(z)$ obtenemos

$$\zeta'(z+a) = \zeta'(z) + \frac{1}{2}\left(\frac{\wp''(z)\Big[\wp(z) - \wp(a)\Big] - \wp'(z)\Big[\wp'(z) - \wp'(a)\Big]}{\Big[\wp(z) - \wp(a)\Big]^2}\right),$$

así que

$$-\wp(z+a) = -\wp(z) + \frac{1}{2}\left(\frac{\wp''(z)\Big[\wp(z) - \wp(a)\Big] - \wp'(z)\Big[\wp'(z) - \wp'(a)\Big]}{\Big[\wp(z) - \wp(a)\Big]^2}\right).$$

Si repetimos lo anterior pero derivando ahora con respecto a a se obtiene

$$-\wp(z+a) = -\wp(a) - \frac{1}{2}\left(\frac{\wp''(a)\Big[\wp(z) - \wp(a)\Big] - \wp'(a)\Big[\wp'(z) - \wp'(a)\Big]}{\Big[\wp(z) - \wp(a)\Big]^2}\right).$$

Sumando las dos ecuaciones que tenemos para $-\wp(z+a)$ tenemos

$$\begin{aligned}
-2\wp(z+a) &= -\wp(z) - \wp(a) + \\
&\quad + \frac{1}{2}\left(\frac{\wp''(z)\Big[\wp(z) - \wp(a)\Big] - \wp'(z)\Big[\wp'(z) - \wp'(a)\Big]}{\Big[\wp(z) - \wp(a)\Big]^2}\right) \\
&\quad - \frac{1}{2}\left(\frac{\wp''(a)\Big[\wp(z) - \wp(a)\Big] - \wp'(a)\Big[\wp'(z) - \wp'(a)\Big]}{\Big[\wp(z) - \wp(a)\Big]^2}\right), \\
-2\wp(z+a) &= -\wp(z) - \wp(a) + \frac{1}{2}\left(\frac{\Big[\wp''(z) - \wp''(a)\Big]\Big[\wp(z) - \wp(a)\Big]}{\Big[\wp(z) - \wp(a)\Big]^2}\right) \\
&\quad - \frac{1}{2}\left(\frac{\Big[\wp'(z) - \wp'(a)\Big]\Big[\wp'(z) - \wp'(a)\Big]}{\Big[\wp(z) - \wp(a)\Big]^2}\right),
\end{aligned}$$

$$-2\wp(z+a) = -\wp(z)-\wp(a)+\frac{1}{2}\left(\frac{\Big[\wp''(z)-\wp''(a)\Big]\Big[\wp(z)-\wp(a)\Big]}{\Big[\wp(z)-\wp(a)\Big]^2}\right) -\frac{1}{2}\left(\frac{\Big[\wp'(z)-\wp'(a)\Big]^2}{\Big[\wp(z)-\wp(a)\Big]^2}\right).$$

Ya que

$$\Big(\wp'(z)\Big)^2 = 4\Big[\wp(z)\Big]^3 - 60G_4\wp(z) + 140G_6,$$

derivando ambos lados obtenemos

$$2\wp'(z)\wp''(z) = 12\Big[\wp(z)\Big]^2\wp'(z) - 60G_4\wp'(z),$$

dividiendo ambos lados de está ecuación entre $2\wp'(z)$ obtenemos

$$\wp''(z) = 6\Big[\wp(z)\Big]^2 - 30G_4 = 6\left(\Big[\wp(z)\Big]^2 - 5G_4\right)$$

si sustituimos el valor de $\wp''(z)$ en la ecuación de $-2\wp(z+a)$ obtenemos

$$\begin{aligned} -2\wp(z+a) &= -\wp(z)-\wp(a)-\frac{1}{2}\left(\frac{\Big[\wp'(z)-\wp'(a)\Big]^2}{\Big[\wp(z)-\wp(a)\Big]^2}\right) \\ &\quad +\frac{6}{2}\left(\frac{\Big[\Big(\wp(z)\Big)^2-5G_4-\Big(\wp(a)\Big)^2+5G_4\Big]\Big[\wp(z)-\wp(a)\Big]}{\Big[\wp(z)-\wp(a)\Big]^2}\right) \\ &= -\wp(z)-\wp(a)-\frac{1}{2}\left(\frac{\Big[\wp'(z)-\wp'(a)\Big]^2}{\Big[\wp(z)-\wp(a)\Big]^2}\right) \\ &\quad +3\left(\frac{\Big[\Big(\wp(z)\Big)^2-\Big(\wp(a)\Big)^2\Big]\Big[\wp(z)-\wp(a)\Big]}{\Big[\wp(z)-\wp(a)\Big]^2}\right) \end{aligned}$$

$$\begin{aligned}
-2\wp(z+a) &= -\wp(z)-\wp(a)+-\frac{1}{2}\left(\frac{\Big[\wp'(z)-\wp'(a)\Big]^2}{\Big[\wp(z)-\wp(a)\Big]^2}\right) \\
&\quad 3\left(\frac{\Big[\wp(z)+\wp(a)\Big]\Big[\wp(z)-\wp(a)\Big]\Big[\wp(z)-\wp(a)\Big]}{\Big[\wp(z)-\wp(a)\Big]^2}\right) \\
&= -\wp(z)-\wp(a)+3\Big[\wp(z)+\wp(a)\Big]-\frac{1}{2}\left(\frac{\Big[\wp'(z)-\wp'(a)\Big]^2}{\Big[\wp(z)-\wp(a)\Big]^2}\right) \\
&= 2\Big[\wp(z)+\wp(a)\Big]-\frac{1}{2}\left(\frac{\Big[\wp'(z)-\wp'(a)\Big]^2}{\Big[\wp(z)-\wp(a)\Big]^2}\right).
\end{aligned}$$

Finalmente dividiendo entre -2 llegamos al resultado deseado

$$\wp(z+a) = -\wp(z)-\wp(a)+\frac{1}{4}\left(\frac{\wp'(z)-\wp'(a)}{\wp(z)-\wp(a)}\right)^2$$

lo cual necesitabamos para demostrar la proposición 5. Debemos notar que cuando a tiende a z la última ecuación tiende a

$$\wp(2z) = -2\wp(z)+\frac{1}{4}\left(\frac{\wp''(z)}{\wp'(z)}\right)^2$$

Con esto terminamos nuestro estudio de las curvas elípticas en el campo complejo.

3.4. CURVAS ELÍPTICAS EN CAMPOS FINITOS

Un caso especial de campos en los que se pueden definir las curvas elípticas son los campos finitos, los cuáles son de nuestro particular interés ya que para la criptografía en curvas elípticas se utilizan la curvas elípticas en este tipo de campos, por lo que, en este capítulo se verán algunas de las propiedades que tendrán las curvas elípticas en campos finitos.

Antes de ver esto veamos algunas definiciones respecto a campos.

DEFINICIÓN 3.4.1 Sea $\mathbb{F}$ un campo. Se define como *la característica de un campo* $\mathbb{F}$ (denotada por $Car(\mathbb{F})$), el mínimo p en $\mathbb{N}$ tal que para algún $a \neq 0$ en $\mathbb{F}$

$$\underbrace{a + a + \cdots + a}_{p \ veces} = pa = 0.$$

OBSERVACIÓN 3.4.2 De esta definición podemos notar que la característica de un campo debe ser un número primo (de ser un número compuesto existirían q y $m \in \mathbb{N}$ tales que $p = qm$, donde $m, q < p$, entonces $pa = mqa = 0$, pero por las propiedades de campo $ma = 0$ o $qa = 0$ en ambos casos concluiríamos que existe un $x \in \mathbb{N}$ que es menor que p tal que $xa = 0$, lo cual contradice el hecho de que p era el mínimo natural que cumple con esta propiedad). Mas aún cuando $\mathbb{F}$ tiene un número primo de elementos (digamos p), entonces $Car(\mathbb{F}) = p$.

Para ver algunas de las propiedades de los campos finitos comencemos tomando un campo finito $\mathbb{F}_p$ con p elementos, en donde p es un número primo, usualmente $\mathbb{F}_p$ es el campo $\mathbb{Z}/\mathbb{Z}_p$, cuando no es este último campo podemos dar un isomorfismo entre $\mathbb{F}_p$ y $\mathbb{Z}/\mathbb{Z}_p$[10]. Aunque es más sencillo trabajar con $\mathbb{Z}/\mathbb{Z}_p$, las propiedades que veremos se definirán en $\mathbb{F}_p$ para hacerlo de manera general.

[10]Teorema 7.3 en la página 362 de [**?**]

Ahora bien, dado el campo $\mathbb{F}_p$ podemos construir una extensión la cuál tenga exactamente p^n elementos[11] para toda $n \in \mathbb{N}$, esta extensión la denotaremos por $\mathbb{F}_{p^n}$. En el caso del campo $\mathbb{Z}/\mathbb{Z}_p$, ésta extensión es $\mathbb{Z}/\mathbb{Z}_{p^n}$.

Podemos notar que al ser $\mathbb{F}_{p^n}$ una extensión de $\mathbb{F}_p$, entonces bajo las operaciones del campo $\mathbb{F}_{p^n}$, éste es un espacio vectorial sobre $\mathbb{F}_p$[12], donde la dimensión de $\mathbb{F}_{p^n}$ sobre $\mathbb{F}_p$ es n, es decir, la dimensión de $\mathbb{F}_{p^n}$ como espacio vectorial sobre $\mathbb{F}_p$ es n. Al hablar de un espacio vectorial uno podría suponer que los elementos de $\mathbb{F}_{p^n}$ son exactamente $n - adas$ ordenadas de elementos de $\mathbb{F}_p$, es decir, elementos de $(\mathbb{F}/\mathbb{F}_p)^n$, pero esto no es así. Esto lo podemos notar con $\mathbb{Z}/\mathbb{Z}_{p^n}$, el cuál esta formado por los elementos del conjunto $\{1, 2, \ldots p^n - 1, p^n\}$ de los cuales ninguno es un elemento de $(\mathbb{Z}/\mathbb{Z}_p)^n$. Sin embargo, analizando el caso general se puede dar el siguiente isomorfismo entre $(\mathbb{F}/\mathbb{F}_p)^n$ y $\mathbb{F}/\mathbb{F}_{p^n}$

$$\begin{aligned} \psi &: (\mathbb{F}/\mathbb{F}_p)^n \to \mathbb{F}/\mathbb{F}_{p^n} \\ \psi(a_1, a_2, \ldots a_n) &= a_1 + a_2 p + \cdots + a_n p^{n-1} \end{aligned}$$

Por otro lado, al ser $\mathbb{F}_{p^n}$ una extensión de $\mathbb{F}_p$, entonces todo $b \in \mathbb{F}_p$ también pertenece a $\mathbb{F}_{p^n}$, entonces $Car(\mathbb{F}_{p^n})$ tiene que ser p.

DEFINICIÓN 3.4.3 Sea G un grupo. Se define como el *orden de el grupo* G (denotado por $o(G)$) al número de elementos que tiene el grupo.

DEFINICIÓN 3.4.4 Sea G un grupo. Tomemos $a \in G$. Definimos *el orden de* a (denotado por $o(a)$) como el mínimo $m \in \mathbb{N}$ tal que $a^m = e$ (en el caso de la suma es $ma = 0$), donde e es el elemento neutro del grupo.

Dos resultados importante relacionados con las definiciones anteriores son los siguientes.

TEOREMA 3.4.5 Sea G un grupo. Para cualquier $a \in G$ tenemos que $o(a)|o(G)$.[13]

[11] Lema 7.4A en la página 363 de [**?**]

[12] scceión 1 en la página 198 de citehe

[13] Corolario 1 en la pág. 51 de [**?**]

TEOREMA 3.4.6 Para cualquier $a \in G$ tenemos que $a^{o(G)} = e$ donde e es el elemento neutro del grupo G.[14]

OBSERVACIÓN 3.4.7 Del último teorema debemos notar que cuando $o(G)$ es un número primo, para cualquier elemento $a \in G$, tendremos cada uno de los elementos a^i (con i en $\{1, 2, \ldots, o(G))$ son distintos (de no ser así $o(a) < o(G)$ por lo que $o(a) \nmid o(G)$). Así, cualquier $a \in G$ es un *generador de* G, es decir, para cualquier $b \in G$ existe $m \in \{1, 2, \ldots o(G)\}$ tal que $a^m = b$.

En el caso de $\mathbb{F}/\mathbb{F}_{p^n}$ sus elementos distintos del neutro aditivo forman un grupo (denotado por $(\mathbb{F}/\mathbb{F}_{p^n})^*$), el cual consta de $p^n - 1$ elementos, por lo que a partir de los últimos teoremas concluimos que para todo $a \in (\mathbb{F}/\mathbb{F}_{p^n})^*$, $\overline{1}a^{p^n-1} = \overline{1}$ donde $\overline{1}$ es el neutro multiplicativo de $(\mathbb{F}/\mathbb{F}_{p^n})^*$, es decir, cada elemento de $(\mathbb{F}/\mathbb{F}_{p^n})^*$ satisface la ecuación $\overline{1}x^{p^n} - \overline{1}x = \overline{0}$, donde $\overline{0}$ es el neutro aditivo del campo. Debemos notar que el polinomio $\overline{1}x^{p^n} - \overline{1}x$ tiene p^n raíces en $\mathbb{F}/\mathbb{F}_{p^n}$ y como $\overline{0}$ es raíz del polinomio, así como también los $p^n - 1$ elementos de $(\mathbb{F}/\mathbb{F}_{p^n})^*$, entonces todas las raíces del polinomio $\overline{1}x^{p^n} - \overline{1}x$ son los elementos de $\mathbb{F}/\mathbb{F}_{p^n}$. Por otro lado, como $\mathbb{Z}/\mathbb{Z}_{p^n}$ y $\mathbb{F}/\mathbb{F}_{p^n}$ son isomorfos podemos ver que los elementos de $\mathbb{Z}/\mathbb{Z}_{p^n}$, también serán las raíces del polinomio $x^{p^n} - x = 0$, utilizando las operaciones en $\mathbb{Z}/\mathbb{Z}_{p^n}$.

Esta información será suficiente por el momento para ver las curvas elípticas en campos finitos, por lo que empezaremos a desarrollar este tema.

Tomemos un campo finito $\mathbb{F}_q$ donde $q = p^r$ y $\mathbb{F}_q$ tiene q elementos, en donde p es un número primo. Sea $\mathbf{E}(\mathbb{F}_q)$ una curva elíptica definida en el campo $\mathbb{F}_q$. Debido a que la característica de un campo debe ser un número primo y divide al número de elementos del campo (por el teorema 3.4.5), entonces la $Car(\mathbb{F}_q) = p$ y la curva $\mathbf{E}$ queda definida por las ecuaciones del tipo:

(a) $y^2 = x^3 + cx^2 + dx + e$, si $Car(\mathbb{F}_q) = 3$

(b) $y^2 = x^3 + dx + e$, si $Car(\mathbb{F}_q) \neq 2, 3$

(c) $y^2 + axy = x^3 + cx^2 + e$, si $Car(\mathbb{F}_q) = 2$ y el coeficiente del termino xy es diferente de cero.

[14] Corolario 2 en la pág. 51 de [**?**]

(d) $y^2 + ay = x^3 + dx + e$, si $Car(\mathbb{F}_q) = 2$ y el coeficiente del termino xy es cero.

LEMA 3.4.8 La curva $\mathbf{E}(\mathbb{F}_q)$ tiene a lo más $2q + 1$ puntos.

DEMOSTRACIÓN.

Sean $x_1, ..., x_q$ los diferentes puntos de $\mathbb{F}_q$. Si hacemos $u_i = x_i^3 + cx_i^2 + dx_i + e$, se pueden obtener a lo más q valores de la forma u_i (aquí c, d ó e podrían ser ceros, dependiendo de la forma que adopta la ecuación de la curva).

Ahora bien, la ecuación $y^2 + ax_iy + by = u_i$ (en donde a o b pueden ser cero, dependiendo de la forma de la ecuación) tiene a lo más dos soluciones para cada valor de u_i. Entonces por cada valor de x_i tenemos a lo más dos valores (y_i y y'_i), tales que (x_i, y_i) y (x_i, y'_i) son soluciones de $y^2 + axy + by = x^3 + cx^2 + dx + e$.

Con lo anterior tenemos a lo más $2q$ parejas $(x, y) \in {\mathbb{F}_q}^2$ que satisfacen la ecuación $y^2 + axy + by = x^3 + cx^2 + dx + e$. Como incluimos a O en $\mathbf{E}(\mathbb{F}_q)$, concluimos que $\mathbf{E}(\mathbb{F}_q)$ tiene a lo más 2q+1 puntos. ■

Con el lema anterior queda demostrado que el número de puntos en $\mathbf{E}(\mathbb{F}_q)$ ($\#(\mathbf{E}(\mathbb{F}_q))$ es a lo más 2q+1. Hay mejores cotas como la que se da en el siguiente teorema, pero la demostración de ellas queda fuera del alcance de esta tesis.

TEOREMA 3.4.9 Teorema de Hasse[15]

Sea N el número de puntos en $\mathbf{E}(\mathbb{F}_q)$, entonces:

$$|N - (q + 1)| \leqslant 2\sqrt{q}$$

Si una curva elíptica $\mathbf{E}$ está definida en $\mathbb{F}_q$ entonces también está definida en $\mathbb{F}_{q^r}$ para cada $r = 1, 2, ...$ y así es significativo considerar los puntos en $\mathbf{E}(\mathbb{F}_{q^r})$, es decir, las soluciones de la ecuación de la curva en los campos de extensión.

[15] Ver Teorema 1.1 en el capítulo 5 de [?]

Si comenzamos con $\mathbb{F}_q$ como el campo en el que $\mathbf{E}$ está definido, denotaremos por N_r el número de puntos en $\mathbf{E}(\mathbb{F}_{q^r})$. Así $N_1 = N$ es el número de puntos que son solución de la curva en $\mathbb{F}_q$.

Con los números N_r formaremos la "serie generadora" $\mathrm{Z(T;\mathbf{E}(\mathbb{F}_q))}$ que es la serie de potencias formal en $Q[[T]]$ definida por:

$$\mathrm{Z(T;\mathbf{E}(\mathbb{F}_q))} = e^{\Sigma N_r \mathrm{T}^r/r},$$

en donde T es una indeterminada, la notación $\mathbf{E}(\mathbb{F}_q)$ designa la curva elíptica y el campo que estamos tomando como base, la suma es bajo todos los números $r = 1, 2, \ldots$. A esta serie le llamaremos la función zeta de la curva elíptica (en $\mathbb{F}_q$) y es un objeto muy importante asociado a $\mathbf{E}$.

Existe una conjetura muy especial llamada la "Conjetura de Weil", para variedades algebraicas de cualquier dimensión, en la cual se ve que la función zeta tiene una forma muy especial.

Cabe mencionar que nuestras curvas elípticas son variedades algebraicas, por lo cual en el caso de curvas elípticas la conjetura de Weil se puede ver como sigue:

CONJETURA 3.4.10 Conjetura de Weil

La función zeta es una función racional de T que tiene la forma

$$\mathrm{Z(T;\mathbf{E}(\mathbb{F}_q))} = \frac{1 - a\mathrm{T} + q\mathrm{T}^2}{(1 - \mathrm{T})(1 - q\mathrm{T})},$$

donde únicamente el entero a depende de la curva elíptica $\mathbf{E}$ en particular. El valor a está relacionado con $N = N_1$, como sigue : $N = q+1-a$. Además el discriminante del polinomio cuadrático en el numerador es negativo (es decir, $a^2 < 4q$ por el Teorema de Hasse) y así el polinomio cuadrático tiene 2 raíces conjugadas complejas α y $\overline{\alpha}$ ambas de norma $\sqrt{q}$ (más precisamente, $1/\alpha$ y $1/\overline{\alpha}$ son las raíces y α y $\overline{\alpha}$ son las "raíces recíprocas").

Si nosotros conocieramos el valor de N, entonces podríamos calcular el valor de cada uno de los N_r de la siguiente manera, por definición:

$$\mathrm{Z(T;\mathbf{E}(\mathbb{F}_q))} = e^{\sum N_r \mathrm{T}^r/r}.$$

Aplicando logaritmo natural a ambos lados de la ecuación:

$$\log(\mathrm{Z}(\mathrm{T};\mathbf{E}(\mathbb{F}_q)) = \sum N_r \mathrm{T}^r/r.$$

Derivando en ambos lados:

$$\frac{d^n}{d\mathrm{T}^n}\log \mathrm{Z}(\mathrm{T};\mathbf{E}(\mathbb{F}_q)) = \frac{d^n}{d\mathrm{T}^n}\left(\sum_{r=1}^{\infty} N_r \mathrm{T}^r/r\right).$$

De donde separando la suma hasta $n-1$, n y de $n+1$ en adelante:

$$\begin{aligned}\frac{d^n}{d\mathrm{T}^n}\log \mathrm{Z}(\mathrm{T};\mathbf{E}(\mathbb{F}_q)) &= \frac{d^n}{d\mathrm{T}^n}(\sum_{r=1}^{n-1}(N_r \mathrm{T}^r/r)) + \frac{d^n}{d\mathrm{T}^n}(N_n \mathrm{T}^n/n) + \\ &\quad + \frac{d^n}{d\mathrm{T}^n}(\sum_{r=n+1}^{\infty}(N_r \mathrm{T}^r/r)).\end{aligned}$$

Calculando las derivadas podemos ver que la primera suma es 0, entonces:

$$\frac{d^n}{d\mathrm{T}^n}\log \mathrm{Z}(\mathrm{T};\mathbf{E}(\mathbb{F}_q)) = \frac{n!}{n}(N_n) + \sum_{r=n+1}^{\infty}\frac{(r-n)!}{n}(N_r \mathrm{T}^{r-n}).$$

Haciendo $i = r-n$ en la última suma, tenemos:

$$\frac{d^n}{d\mathrm{T}^n}\log \mathrm{Z}(\mathrm{T};\mathbf{E}(\mathbb{F}_q)) = \frac{n!}{n}(N_n) + \sum_{i=1}^{\infty}\frac{(i)!}{n}(N_{i+n} \mathrm{T}^i),$$

finalmente al evaluar en T=0:

$$\frac{d^n}{d\mathrm{T}^n}\log \mathrm{Z}(\mathrm{T};\mathbf{E}(\mathbb{F}_q))|_{T=0} = \frac{n!}{n}(N_n) + (\sum_{i=1}^{\infty}\frac{i!}{n}(N_{i+n} \mathrm{T}^i))|_{T=0}.$$

Como la última suma es 0, obtenemos:

$$\frac{d^n}{d\mathrm{T}^n}\log \mathrm{Z}(\mathrm{T};\mathbf{E}(\mathbb{F}_q))|_{T=0} = \frac{n!}{n}(N_n).$$

Despejando N_n:

$$N_n = \frac{1}{(n-1)!}\frac{d^n}{d\mathrm{T}^n}\log \mathrm{Z}(\mathrm{T};\mathbf{E}\big(\mathbb{F}_q)\big)|_{T=0}.$$

Pero, si fuera cierta la conjetura de Weil, entonces

$$\mathrm{Z}(\mathrm{T};\mathbf{E}(\mathbb{F}_q)) = \frac{1-a\mathrm{T}+q\mathrm{T}^2}{(1-\mathrm{T})(1-q\mathrm{T})} = \frac{(1-\alpha\mathrm{T})(1-\overline{\alpha}\mathrm{T})}{(1-\mathrm{T})(1-q\mathrm{T})},$$

sustituyendo en la formula anterior:

$$N_n = \frac{1}{(n-1)!}\frac{d^n}{d\mathrm{T}^n}\log\left(\frac{(1-\alpha\mathrm{T})(1-\overline{\alpha}\mathrm{T})}{(1-\mathrm{T})(1-q\mathrm{T})}\right)\Bigg|_0.$$

De donde, separando los logaritmos tenemos:

$$N_n = \frac{1}{(n-1)!}\frac{d^n}{d\mathrm{T}^n}\Big(\log(1-\alpha\mathrm{T})+\log(1-\overline{\alpha}\mathrm{T})-\log(1-\mathrm{T})-\log(1-q\mathrm{T})\Big)\Bigg|_0.$$

Dado que $\log(1-\mathrm{T}) = -\mathrm{T}-\frac{\mathrm{T}^2}{2}-\frac{\mathrm{T}^3}{3}-\frac{\mathrm{T}^4}{4}...$, sustituyendo tenemos que:

$$N_n = \frac{1}{(n-1)!}\frac{d^n}{d\mathrm{T}^n}\left(-\sum_{i=1}^{\infty}\frac{(\alpha\mathrm{T})^i}{i}-\sum_{i=1}^{\infty}\frac{(\overline{\alpha}\mathrm{T})^i}{i}+\sum_{i=1}^{\infty}\frac{(\mathrm{T})^i}{i}+\sum_{i=1}^{\infty}\frac{(q\mathrm{T})^i}{i}\right)\Bigg|_0.$$

Como, si $i<n$, entonces $\frac{d^n}{d\mathrm{T}^i}=0$ y, si $i\geqslant n$, tenemos $\frac{d^n}{d\mathrm{T}^n} = i(i-1)...(i-n+1)\mathrm{T} = \frac{i!}{(i-n)!}\mathrm{T}^{i-n}$ por lo cual al derivar, los primeros n-1 términos son cero.

Asi derivando obtenemos:

$$\begin{aligned} N_n &= \frac{1}{(n-1)!}\left(-\sum_{i=n}^{\infty}\frac{i!}{(i-n)!}\frac{\alpha^i}{i}\mathrm{T}^{i-n}-\sum_{i=n}^{\infty}\frac{i!}{(i-n)!}\frac{\overline{\alpha}^i}{i}\mathrm{T}^{i-n}\right. \\ &\quad \left.+\sum_{i=n}^{\infty}\frac{i!}{(i-n)!}\frac{1}{i}\mathrm{T}^{i-n}+\sum_{i=n}^{\infty}\frac{i!}{(i-n)!}\frac{q^i}{i}\mathrm{T}^{i-n}\right)\Bigg|_0. \end{aligned}$$

Ahora bien para todo $i>n$ $\quad \mathrm{T}^{i-n}\big|_0 = 0$ y cuando $i=n$ $\quad \mathrm{T}^{i-n}\big|_0 = 1$ por lo cual:

$$\begin{aligned} N_n &= \frac{1}{(n-1)!}\left(-\frac{n!}{(n-n)!}\frac{\alpha^n}{n}\mathrm{T}^{n-n}-\frac{n!}{(n-n)!}\frac{\overline{\alpha}^n}{n}\mathrm{T}^{n-n}\right. \\ &\quad \left.+\frac{n!}{(n-n)!}\frac{1}{n}\mathrm{T}^{n-n}+\frac{n!}{(n-n)!}\frac{q^n}{n}\mathrm{T}^{n-n}\right)\Bigg|_0. \end{aligned}$$

Por lo cual:

$$N_n = \frac{1}{(n-1)!}\left(-(n-1)!\alpha^n - (n-1)!\overline{\alpha}^n + (n-1)! + (n-1)!q^n \right).$$

Finalmente:

$$N_n = q^n + 1 - \alpha^n - \overline{\alpha}^n.$$

Con lo cual tenemos finalmente el valor de N_n.

Hasta el momento solamente tenemos acotado el número de puntos en la curva elíptica o como en el último caso una ecuación para este número, pero apartir de otros datos que no necesariamente conocemos. En la sección 4.5 se dará un método de tipo exponencial para el cálculo del número de puntos en una curva elt́ipica.

Con esto terminamos nuestra revisión por las curvas elípticas. Daremos paso ahora a ver una de las aplicaciones de las curvas elípticas.

Capítulo 4

CURVAS ELÍPTICAS EN CRIPTOGRAFÍA

4.1. INTRODUCCIÓN

Después de haber visto las fórmulas que definen la suma en una curva elíptica, se puede uno imaginar que el siguiente problema es difícil:

Si en una curva elíptica se conocen P y kP (donde k es un entero y kP significa sumar k veces el elemento P, si k es positivo y $|k|$ veces $-P$, si k es negativo), es muy difícil conocer k.

Éste se conoce como el *Problema del Logaritmo Discreto*. Este problema ha sido muy estudiado, pero los únicos algoritmos que se conocen para resolver este problema son en tiempo exponencial, por lo que se puede usar esta hecho para aplicarlo a la criptografía.

La estructura de grupo que le dimos a una curva elíptica, en la sección anterior, se puede dar, exactamente en la misma manera en cualquier campo que no tenga característica 2 o 3. Nos concentramos en los reales porque éso

nos permitió tener una idea geométrica, pero si usted observa las fórmulas obtenidas, verá que son válidas en cualquiera de los campos mencionados.

El uso de las curvas en criptografía no ha sido implementado para ser usado ampliamente, como ocurre con el sistema RSA. Ahora describiremos cómo se aplica.

4.2. ASIGNACIÓN DE UN PUNTO EN LA CURVA ELÍPTICA A UNA UNIDAD DE MENSAJE

En principio cualquiera supondría que al querer hacer una encriptación en una curva elíptica, deberíamos de escoger primero la curva sobre la cual vamos a trabajar y dar la ecuación de la curva, pero esto no ocurre así, debido a que el mensaje que deseamos cifrar está compuesto por unidades de mensaje (las cuales pueden ser de tamaño 1, es decir, que consten de un solo símbolo o de tamaño n es decir que cada unidad de mensaje tenga n símbolos), y sería deseable que a cada unidad de mensaje que quisieramos encriptar le correspondiera un punto en la curva. En el teorema 3.4.9 comentamos el Teorema de Hasse, el cual nos dice que si tenemos una curva elíptica definida en un campo $\mathbb{F}_q$, entonces el número de puntos (N), de la curva cumple las siguientes desigualdades

$$q + 1 - 2\sqrt{q} \leqslant N \leqslant q + 1 + 2\sqrt{q}$$

esto sin importar la ecuación que tenga la curva. Por lo que si nuestro mensaje tiene un cierto número m de unidades de mensaje distintas, entonces para asegurarnos que a cada unidad de mensaje le corresponda un punto en la curva elíptica necesitaremos que

$$m < q + 1 - 2\sqrt{q} \leqslant N$$

por esto queda claro que es preferible ocuparnos primero de las unidades de mensaje y posteriormente del número q con el cual definiremos el campo $\mathbb{F}_q$. Debido a lo anterior nos ocuparemos primero de las unidades de mensaje.

Trabajar con las unidades de mensaje resultaría algo incomodo, por lo que haremos primero una asociación entre cada unidad de mensaje y algún

número natural, para de esta forma trabajar con números en lugar de con unidades de mensaje. A cada unidad de mensaje le asociaremos aleatoriamente un número $u \in \mathbb{N}$, únicamente nos fijaremos en que a dos unidades de mensaje distintas no les corresponda el mismo número. Para denotar a las unidades de mensaje en general usaremos el símbolo α.

Unidad de mensaje		Número natural
α	$\longrightarrow$	u

Ya que hemos asociado un número a cada unidad de mensaje, el paso siguiente será asignar a cada uno de estos números un punto en una curva elíptica que estará definida en un campo $\mathbb{F}_q$. Aquí nos enfrentamos con dos problemas, el primero es saber cuál es la ecuación de la curva elíptica y el segundo saber quién es $\mathbb{F}_q$. Por el momento no estamos en condiciones de dar respuesta a ninguna de estas 2 cuestiones, sin embargo, podemos trabajar en abstracto con una curva elíptica $\mathbf{E}(\mathbb{F}_q)$, que esté definida por una ecuación de la forma $y^2 = x^3+ax^2+bx+c$ y tratar de encontrar condiciones adecuadas que deban cumplir $\mathbb{F}_q$, a, b y c de tal manera que la curva que encontremos sirva para nuestros propósitos.

Como lo mencionamos antes desearíamos que cada unidad de mensaje tuviera asociado un punto en la curva, y ya que cada unidad de mensaje tiene asociado un número natural, nos será más facil asociarle a cada uno de estos números un punto en la curva, como se muestra en el siguiente diagrama.

Unidad de mensaje		Número natural		Punto en la curva
α	$\longrightarrow$	u	$\longrightarrow$	P

Sería deseable que esto no se haga de una manera aleatoria, sino de una manera ordenada y además sencilla, para que si nosotros tomamos un punto

P en la curva podamos encontrar fácilmente el número natural correspondiente u y por tanto recuperar la unidad de mensaje α asociada a ese punto. Y viceversa, si nosotros tomamos una unidad de mensaje de nuestro texto, ya que sepamos cuál es el número natural u que le corresponde, entonces podamos calcular rápidamente cuál será el punto P que le corresponde en la curva.

Para el problema de asignar un punto de la curva a un número existen varios métodos de solución, el que describiremos a continuación es un método de tipo probabilístico. Para comenzar tomaremos un número $k \in \mathbb{N}$, es importante que este número k sea un número grande ya que de la elección de este número dependerá la probabilidad de que el método funcione o no, como se explicará posteriormente.

A continuación busquemos un número M tal que para cualquier número u asignado a una unidad de mensaje ocurra que $u < M$ y consideremos el número Mk. Cada número mayor que 1 pero menor que Mk dividámoslo entre k para obtener un cociente a y un residuo j, los cuales cumplirán que $0 \leqslant a < M$ y $0 \leqslant j < k$. De manera que, si $u \in \mathbb{N}$ es tal que $1 \leqslant u < Mk$, entonces:

$$u = ak + j$$

Debemos mencionar un hecho importante, debido a que si una unidad de mensaje tiene asociado un número u ($u < M$), entonces de entre los números que se encuentran entre 1 y Mk existirán algunos que al dividirlos por k tendrán como cociente a u, de hecho, éstos son los k números que se escriben en la forma

$$uk + j \qquad \text{con} \quad 0 \leqslant j < k$$

este paso es importante, porque recordemos que deseabamos asignar a un número u (el cual correspondia a una unidad de mensaje) un punto en la curva, con el paso anterior cada número u lo podemos relacionar ahora con k números (aquellos que tienen como cociente u, como resultado de dividirlos por k) esto nos será de utilidad posteriormente.

Unidad de mensaje		Número natural		Números asociados
			$\longrightarrow$	uk
			$\longrightarrow$	$uk+1$
α	$\longrightarrow$	u	$\vdots$	$\vdots$
			$\longrightarrow$	$uk+(k-2)$
			$\longrightarrow$	$uk+(k-1)$

El siguiente paso será asociar, a cada número u entre 1 y Mk, algún elemento x_n que se encuentre en $\mathbb{F}_q$, recordemos que cada punto P en la curva elíptica, es de la forma (x_P, y_P) donde x_P, $y_P \in \mathbb{F}_q$, de tal manera que si tenemos al elemento x_u podemos tratar de ver si existe algún punto $a \in \mathbb{F}_q$ tal que (x_u, a) esté en la curva elíptica y entonces hacer $y_u = a$.

Pero vayamos paso a paso. Para el problema de cómo asociarle un elemento de $\mathbb{F}_q$ a cada u, recordemos que en la sección 3.4 se menciono que existe una manera de hacer una correspondencia entre $\mathbb{F}_q$ y $\mathbb{Z}_q$ (la cual no se dio pero se dio una referencia en la nota 10 pág. 84). De tal manera que a cada elemento $z \in \mathbb{Z}_q$ se le puede asociar un elemento $x \in \mathbb{F}_q$, y como $\mathbb{Z}_q = \{1, ..., q\}$, entonces todo número natural u que satisfaga $1 \leqslant u < Mk$, cumplirá que $u \in \mathbb{Z}_q$ por lo que podremos encontrar un elemento $x_u \in \mathbb{F}_q$ asociado a u.

Número natural		Número en $\mathbb{Z}_q$		Elemento en $\mathbb{F}_q$
u	$\longrightarrow$	u	$\longrightarrow$	x_u

Ahora bien, como ya vimos cada uno de estos números u lo podemos escribir en la forma $u = ak + j$ con $1 \leqslant a < M$ y $0 \leqslant j < k$. Con está identificación entonces podemos renombrar el valor asociado a u en $\mathbb{F}_q$ por x_{a_j}.

Número natural		Número en $\mathbb{Z}_q$		Elemento en $\mathbb{F}_q$
u	$\longrightarrow$	$u = ak + j$	$\longrightarrow$	x_{a_j}

En sí, no estamos cambiando el elemento asignado a u en $\mathbb{F}_q$, sólo estamos cambiándole el nombre, en lugar de llamarlo x_u lo llamamos ahora x_{a_j}.¿Por qué este cambio de nombre?, es sencillo las unidades de mensaje α tienen asignado un número u y como vimos cada u tendrá asignados k números de la forma $uk + j$, pero por el paso anterior cada uno de estos números $uk + j$ tiene asignado un elemento $x_{u_j} \in \mathbb{F}_q$. De tal manera que a cada número u le asociaremos k elementos en $\mathbb{F}_q$

Unidad de mensaje		Número natural asociado a la unidad de mensaje		Naturales asociados
α	$\longrightarrow$	u	$\longrightarrow$	uk $uk+1$ $\vdots$ $uk+(k-2)$ $uk+(k-1)$

Naturales asociados a cada natural		Número $\mathbb{Z}_q$		Elemento en $\mathbb{F}_q$
uk	$\longrightarrow$	uk	$\longrightarrow$	x_{u_0}
$uk+1$	$\longrightarrow$	$uk+1$	$\longrightarrow$	x_{u_1}
$\vdots$	$\longrightarrow$	$\vdots$	$\longrightarrow$	$\vdots$
$uk+(k-2)$	$\longrightarrow$	$uk+(k-2)$	$\longrightarrow$	$x_{u_{k-2}}$
$uk+(k-1)$	$\longrightarrow$	$uk+(k-1)$	$\longrightarrow$	$x_{u_{k-1}}$

Anteriormente, cuando decidimos asociarle a cada número u, k números debió surgir una pregunta muy natural ¿Para qué asociarle a cada unidad

de mensaje k elementos en $\mathbb{F}_q$, si anteriormente habíamos dicho que sólo necesitabamos asociarle un elemento? En efecto sólo deseamos asociarle un elemento en $\mathbb{F}_q$ a cada unidad de mensaje, desafortunadamente no podremos asegurar que si nosotros tomamos un elemento en $x \in \mathbb{F}_q$ podamos encontrar otro elemento $y \in \mathbb{F}_q$ tal que $(x, y) \in \mathbf{E}(\mathbb{F}_q)$. Esto debido a que la ecuación de la curva es de la forma $y^2 = x^3 + ax^2 + bx + c$ entonces $y = \sqrt{x^3 + ax^2 + bx + c}$, pero recordemos que, por lo visto en la sección de curvas elípticas en un campo finito (enlademostración del Lema 3.4.8), a lo más la mitad de los elementos en el campo tendrán una raíz cuadrada. De tal manera que si a cada u sólo le asociamos un elemento en $\mathbb{F}_q$ (digamos w) puede que no podamos encontrar otro elemento $v \in \mathbb{F}_q$ tal que $v = \sqrt{w^3 + aw^2 + bw + c}$, por lo que tendríamos que reiniciar todo el proceso.

Sin embargo, al asociarle k elementos en $\mathbb{F}_q$ a cada unidad de mensaje tenemos k posibilidades de que para alguno de estos elementos (supongamos x_{u_i}) podamos encontrar un elemento $v \in \mathbb{F}_q$ tal que $v^2 = x_{u_i}^3 + ax_{u_i}^2 + bx_{u_i} + c$. Así podríamos asociarle a u (que tiene asociada la unidad de mensaje α) el punto $P_u = (x_{u_i}, v)$ en la curva elíptica. El procedimiento para encontrar v será de manera exhaustiva, es decir, exploraremos todos los valores u_i hasta encontrar a v de la manera siguiente.

De inicio tomaremos la función $f(x) = x^3 + ax^2 + bx + c$. Tomaremos el primer elemento asociado con u, es decir, para $j = 0$ tomaremos x_{u_j}, y sustituiremos x_{u_j} en $f(x)$ para encontrar $f(x_{u_j})$. Posteriormente buscaremos la raíz cuadrada de $f(x_{u_j})$ en $\mathbb{F}_q$, si encontramos está raíz, entonces definimos $x_u = x_{u_j}$ y $y_u = \sqrt{f(x_{u_j})}$. Si $f(x_{u_j})$ no tiene una raíz cuadrada en $\mathbb{F}_q$ repetimos el proceso con $j = 1$, es decir si $f(x_{u_j})$ tiene una raíz entonces hacemos $y_u = \sqrt{f(x_{u_j})}$. Si $f(x_{u_j})$ no tiene una raíz cuadrada en $\mathbb{F}_q$ con $j = 1$, repetimos el proceso con $j = 2$ y así sucesivamente hasta $j = k$. Si en algún momento pudimos encontrar el elemento $y_u \in \mathbb{F}_q$, entonces definimos $P_u = (x_u, y_u)$ y diremos que este punto será el punto asociado a el natural u en la curva elíptica. Este procedimiento deberemos repetirlo para cada número u asociado con alguna unidad de mensaje.

Naturales asociados a cada natural		Número $\mathbb{Z}_q$		Elemento en $\mathbb{F}_q$	$f(x_{u_j})$ tiene raíz
ua	$\longrightarrow$	ua	$\longrightarrow$	x_{u_0}	$\times$
$ua+1$	$\longrightarrow$	$ua+1$	$\longrightarrow$	x_{u_1}	$\times$
$\vdots$	$\longrightarrow$	$\vdots$	$\longrightarrow$	$\vdots$	$\vdots$
$ua+l$	$\longrightarrow$	$ua+l$	$\longrightarrow$	x_{u_l}	$\checkmark$
$\vdots$	$\longrightarrow$	$\vdots$	$\longrightarrow$	$\vdots$	
$ua+(k-2)$	$\longrightarrow$	$ua+(k-2)$	$\longrightarrow$	$x_{u_{k-2}}$	
$ua+(k-1)$	$\longrightarrow$	$ua+(k-1)$	$\longrightarrow$	$x_{u_{k-1}}$	

Unidad de mensaje		Número natural asociado a la unidad de mensaje		Natural asociado finalmente a la unidad de mensaje		Número $\mathbb{Z}_q$
α	$\longrightarrow$	u	$\longrightarrow$	$ua+l$	$\longrightarrow$	$ua+l$

Unidad de mensaje		Número $\mathbb{Z}_q$		Elemento en $\mathbb{F}_q$		Punto en la curva
α	$\longrightarrow$	$ua+l$	$\longrightarrow$	x_{u_l}	$\longrightarrow$	$(x_{u_l}, \sqrt{f(x_{u_l})})$

Con este procedimiento podremos encontrar para cada unidad de mensaje un punto en la curva.

En un principio mencionamos que este procedimiento era de tipo probabilístico, esto se va a deber a que la probabilidad de no encontrar una raíz de algún elemento $z \in \mathbb{F}_q$ será $N/2q$. Debido a esto la probabilidad de no encontrar una raíz de entre un conjunto de k elementos en $\mathbb{F}_q$ será $(N/2q)^k$,

pero $N/2q < 1/2$ por lo que $(N/2q)^k < (1/2)^k$. Por lo que la probabilidad de no encontrar una raíz dentro de un conjunto de k elementos en $\mathbb{F}_q$ será menor que $1/2^k$, de tal manera que como en un principio tomamos un k muy grande, entonces esta probabilidad será muy cercana a 0, con lo que el método tendrá menos posibilidades de fallar. Aún así, si en algún momento no podemos encontrar la raíz cuadrada de $f(x_{u_j})$ para algún u y toda j con $0 \leqslant j < k$, entonces tendremos que escoger otra curva elíptica o cambiar el campo $\mathbb{F}_q$ sobre el cual estamos trabajando.

Una vez que hemos podido asociar a cada unidad de mensaje un punto en la curva, nos enfrentamos al problema de que, si nosotros tenemos un punto en la curva, ¿Como podremos encontrar la unidad de mensaje correspodiente?

Recordemos que tenemos una manera de asociarle a un número u en $\mathbb{Z}_q$ un elemento x_u en $\mathbb{F}_q$, del mismo modo si tenemos x_u podemos recuperar el valor u. Ahora bien, si tenemos un punto P en la curva éste debe tener coordenadas (x_P, y_P), si tomamos x_P podemos encontrar el número asociado en $\mathbb{Z}_q$ llamémosle n_P, éste número al dividirlo entre k nos dará un cociente u y un residuo i, es decir, $n_P = uk + i$, por lo que u es la parte entera de n_P/k, esto es,

$$u = \left[\frac{n_P}{k}\right]$$

y sabiendo cuál es el natural u entonces podemos recuperar la unidad de mensaje.

Recordemos que todo este procedimiento lo estuvimos haciendo en abstracto ya que no dimos condiciones sobre q para poder definir el campo $\mathbb{F}_q$ sobre el cual quedará definida nuestra curva, ni la ecuación de la misma. Anteriormente mencionamos que para cada número n entre 1 y Mk necesitariamos que $q = \#(\mathbb{F}_q) > n$, lo cual es una restricción sobre q y en sí es la única que tiene q en todo el proceso. Debido a ello necesitaremos que q cumpla con $Mk < q$. Con esto bastará para poder definir $\mathbb{F}_q$ ya que recordemos que el número de elementos de $\mathbb{F}_q$ es exactamente q.

Para el problema de cómo definir la ecuación de la curva elíptica, es decir, encontrar a, b y c para $y^2 = x^3 + ax^2 + bx + c$ necesitaremos primero que a, b y c estén en $\mathbb{F}_q$ y posteriormente que el discriminante del polinomio (es decir, $b^2a^2 - 4ca^3 - 4b^3 + 18cba - 27c^2$) sea distinto del cero de $\mathbb{F}_q$, con lo

cual garantizaremos que el polinomio no tiene raíces multiples y la ecuación $y^2 = x^3 + ax^2 + bx + c$ es la de una curva elíptica.

Con esto terminaremos el problema de como asociar cada unidad de mensaje con algún punto en la curva elíptica. Aquí debemos reflexionar en algo, estamos pidiendo que la curva elíptica esté definida bajo un campo $\mathbb{F}_q$, el tiempo que nos llevamos en hacer el proceso anterior lo podemos reducir significativamente si simplemente elegimos como campo a $\mathbb{Z}_q$, ya que nos ahorraríamos el paso de mandar cada elemento en $\mathbb{Z}_q$ a algún elemento en $\mathbb{F}_q$. Decidí describir el caso general para mostrar el desarrollo completo, sin embargo, para los ejemplos que se desarrollaran a continuación utilizaremos $\mathbb{Z}_q$ en lugar de $\mathbb{F}_q$.

Ejemplo

Aquí veremos como construir una curva elíptica en la cual a cada punto de ésta podamos asociarle una unidad de mensaje, las cuales estarán dadas por las letras del alfabeto, es decir, A,...,Z, por lo que el número de unidades de mensaje (m) será de 27. Para no hacer demasiado largos los cálculos daremos la siguiente correspondencia entre las unidades de mensaje y los naturales.

Texto Plano	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Ordinal	0	1	2	3	4	5	6	7	8	9	10	11	12	13

Texto Plano	$\tilde{N}$	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ordinal	14	15	16	17	18	19	20	21	22	23	24	25	26

A continuación escogeremos $k = 20$ y $M = 36$, como $Mk = 20 * 36 = 720$ escogeremos $q = 751$ el cual es un número primo. Con esto tendremos que el campo que tomaremos será $\mathbb{Z}_{751}$. Sin importarnos la ecuación de la curva que tomemos sabemos por el Teorema de Hasse (Teorema 3.4.9) que dado el campo (En este ejemplo $\mathbb{Z}_{751}$) el número de puntos (N) cumplirá que

$$\begin{aligned} q+1-2\sqrt{q} \leqslant\ & N & \leqslant q+1+2\sqrt{q} \\ 751+1-2\sqrt{751} \leqslant\ & N & \leqslant 751+1+2\sqrt{751} \\ 752-2(27{,}40) \leqslant\ & N & \leqslant 752+2(27{,}40) \\ 752-54{,}80 \leqslant\ & N & \leqslant 752+54{,}80 \\ 724{,}6 \leqslant\ & N & \leqslant 806{,}8 \end{aligned}$$

Lo cual nos dice que, sin importar la ecuación de la curva, ésta tendrá al menos 724 puntos y como nosotros nada más necesitamos 26, tendremos un número suficiente de puntos en la curva para asociarle por lo menos uno de éstos a cada unidad de mensaje. Ahora bien, la ecuación de la curva que escogeremos será $y^2 = x^3 - x + 188$, recordando que la ecuación del discriminante de un polinomio de grado 3 de la forma $x^3 + a_2x^2 + a_1x + a_0$ es

$$a_1^2a_2^2 - 4a_0a_2^3 - 4a_1^3 + 18a_0a_1a_2 - 27a_0^2$$

tendremos que, de acuerdo a la ecuación que escogimos, ésta tiene discriminante

$$\begin{aligned} & (1)^2(0)^2 - 4(188)(0)^3 - 4(1)^3 + 18(188)(1)(0) - 27(188)^2 \\ = \ & -4 - 954288 = -954292 \equiv 229 \pmod{751} \end{aligned}$$

como 229 es distinto de cero módulo 751, entonces aseguramos que el polinomio $x^3 - x + 188$ no tiene raíces multiples, con lo que la ecuación que escogimos sí corresponde a una curva elíptica.

El siguiente paso será ver cuáles son los puntos que hay en la curva. Al final del capítulo se encuentran tres tablas con el fin de ayudarnos con este problema, en la primera se da el número en $\mathbb{Z}_{751}$ y a continuación el resultado que se obtiene al sustituir este número en $x^3 - x + 188$ el resultado se da módulo 751. En la segunda se dan primeramente los números en $\mathbb{Z}_{751}$ seguidos del resultado que se obtiene de sustituir este número en y^2 mod 751. En la última tabla se dan los puntos en la curva elíptica, en la cual además, hemos agregado el punto (∞, ∞) el cual es el $0 \in \mathbf{E}(\mathbb{Z}_{751})$. Estas tablas serán de gran ayuda ya que todos los ejemplos que se den en lo subsecuente se referirán a la curva elíptica que acabamos de definir.

Una vez que hemos definido la curva y todos los valores relacionados con ella, será prudente ver cómo se hace la asociación entre los naturales asociados a la unidad de mensaje y los puntos en la curva elíptica, como ejemplo veremos el caso cuando $u = 3$ que corresponde a la letra D. Para poder realizar esto nos apoyaremos en las tablas 1 y 2.

Como habíamos visto previamente el número u tiene asociados k elementos en $\mathbb{Z}_q$, en nuestro ejemplo serán 20 elementos, los cuales son:

$$60,\ 61,\ \ldots,\ 78,\ 79$$

tomemos el primer elemento, es decir, 60. De acuerdo a la tabla 1, $60^3+60 \equiv 591 \pmod{751}$, con esto buscaremos en la tabla 2 si algún elemento y en $\mathbb{Z}_{751}$ arroja como resultado 591 al hacer $y^2 \pmod{751}$. Desafortunadamente ningún número en $\mathbb{Z}_{751}$ arroja este resultado al hacer la operación, por lo que probaremos con el 61. Para 61 tenemos $61^3 + 61 \equiv 306 \pmod{751}$, pero tampoco ningún elemento en $\mathbb{F}_{751}$ arroja como resultado 306 en la tabla 2.

Sin embargo para 62 tenemos que $62^3 + 62 \equiv 695 \pmod{751}$ para el cual 161 y 590 arrojan como resultado 695 al sustituirlos en $y^2 \pmod{751}$. Notemos que $161 + 590 \equiv 751 \equiv 0 \pmod{751}$ por lo que $161 \equiv -590 \equiv \pmod{751}$, es decir, 161 es el inverso aditivo de 590 en $\mathbb{Z}_{751}$. Con lo que obtenemos que al número 3 le podemos asociar los puntos en la curva $(62, 161)$ o $(62, 590)$, aquí elegimos a $(62, 161)$. De esta manera tenemos que la letra D tiene asociado al punto $(62, 161)$ en la curva elíptica. De manera análoga podemos encontrar los restantes 26 puntos que aparecen en la tabla 4.

4.3. ANALOGÍAS ENTRE $\mathbb{F}_q$ Y E

Una vez que tenemos la curva y los puntos que vamos a utilizar podemos ver cómo haremos la encriptación. Comenzaremos por decir que el campo $\mathbb{Z}_q$ y la curva elíptica **E** definida en algún campo son muy semejantes desde cierto punto de vista. Si el campo $\mathbb{Z}_q$ lo vemos con respecto a la multiplicación veremos que cumple ciertas propiedades.

1)	Elemento neutro	1
2)	Cerradura	$a * b \in \mathbb{F}_q \quad \forall a, b \in \mathbb{Z}_q$
3)	Conmutatividad	$a * b = b * a \quad \forall a, b \in \mathbb{Z}_q$
4)	Asociatividad	$(a * b) * c = a * (b * c) \quad \forall a, b, c \in \mathbb{Z}_q$

Si vemos la curva elíptica y como operación a la suma tendremos

1)	Elemento neutro	$0 \in \mathbb{F}_q$
2)	Cerradura	$P + Q \in \mathbb{F}_q \quad \forall P, Q \in \mathbb{F}_q$
3)	Conmutatividad	$P + Q = Q + P \quad \forall P, Q \in \mathbb{F}_q$
4)	Asociatividad	$(P + Q) + R = P + (Q + R) \quad \forall P, Q, R \in \mathbb{F}_q$

Si en $\mathbb{Z}_q$ tenemos la multiplicación de dos elementos en $\mathbf{E}$ tenemos la suma de dos elementos, si en $\mathbb{Z}_q$ tenemos la multiplicación k veces de un elemento en $\mathbf{E}$ tenemos la suma k veces de un punto en P. Hacemos mencion de esto ya que todos los métodos de encriptación que se vieron en el capítulo están relacionados con la operación *mod* q, que es básicamente trabajar con $\mathbb{Z}_q$ y debido a las analogías que tenemos entre $\mathbb{Z}_q$ y $\mathbf{E}$ trataremos de recuperar algunos de esos métodos con curvas elípticas.

4.4. SUMA DE UN PUNTO EN E, k VECES

En algún momento dado nos importará ver cual es el orden de un punto $P \in \mathbf{E}(\mathbb{F}_q)$ en una curva elíptica, es decir, encontrar la mínima k positiva tal que $kP = 0$. Debido a esto será importante saber cómo sumar un punto k veces. Comencemos por tomar un número n cualquiera, y digamos que dado $P \in \mathbf{E}$ queremos encontrar el punto correspondiente a nP en $\mathbf{E}$. Aquí tomaremos dos casos

1. n es impar

   Si el número es impar entonces, haremos $m = n - 1$ y buscaremos el punto mP para construir el punto $P + mP$ en la curva

2. n es par

   Si el número es par entonces, tomaremos $m = n/2$ y buscaremos el punto mP para una vez que lo hayamos encontrado construir el punto $2(mP)$ en la curva

en ambos casos para encontrar el punto mP se repetira el proceso proceso anterior hasta encontrar que o bien que $m = 0$ para el primer caso o $m = 1$ si estamos en el segundo caso.

Por ejemplo tomemos nuestra curva $y^2 = x^3 - x + 188$ y tomemos un punto en ella digamos $P = (1, 375)$ y busquemos $100P$. Como 100 es par entonces haremos $100P = 2(50P)$ por el inciso 2, A continuación como 50 es par entonces por el inciso 2 tendremos $50P = 2(25P)$, por lo que $100P = 2(2(25P))$. Como 25 es impar entonces en este paso usaremos el inciso 1, por lo que $25P = P + 24P$, luego entonces $100P = 2(2(P + 24P))$. Si seguimos sucesivamente con el procedimiento tendremos que:

$$100P = 2(2(P + 2(2(2(P + 2P)))))$$

el procedimiento de los calculos se muestra en la siguiente tabla en donde se toma $P = (1, 375)$

Algoritmo	Ejemplo
$2P$	(2 , 378)
$P + 2P$	(6 , 361)
$2(P + 2P)$	(207 , 536)
$2(2(P + 2P))$	(180 , 408)
$2(2(2(P + 2P)))$	(513 , 610)
$P + 2(2(2(P + 2P)))$	(296 , 245)
$2(P + 2(2(2(P + 2P))))$	(19 , 138)
$2(2(P + 2(2(2(P + 2P)))))$	(447 , 448)

Antes de ver los métodos de encriptación será importante hacer mención de que los métodos que veremos están basados en los problemas del logaritmo discreto y el de la descomposición en factores primos de un número cualquiera, en particular para el problema del logaritmo discreto será importante analizar primero cuál sería el problema análogo en curvas elípticas.

4.5. CÁLCULO DEL NÚMERO DE PUNTOS EN UNA CURVA ELÍPTICA

Existen varios métodos para calcular el número de puntos en una curva elíptica, en particular aquí mostraremos el llamado "Paso-Pequeño-Paso Gigante". La idea del algoritmo está basada en el Teorema de Hasse (Teorema 3.4.8).

En este algoritmo se elige un punto $P \in \mathbf{E}(\mathbb{F}_q)$ aleatoriamente y se calcula, para cada entero m en el intervalo $(p+1-2\sqrt{q}, p+1+2\sqrt{q})$ el punto mP (recordemos que el número de puntos en la curva elíptica, es decir, N estará también en este intervalo, además de que $NQ = 0$ para todo $Q \in \mathbf{E}(\mathbb{F}_q)$). Si solamente para uno de estos números m tenemos que $mP = 0$, esto nos dirá que este número deberá coincidir con N, es decir, $m = N$, con lo cual habremos encontrado el valor exacto del número de puntos en la curva.

Debido a lo anterior calcularemos mP para todo m en el intervalo $(p+1-2\sqrt{q}, p+1+2\sqrt{q})$, para ello haremos dos pasos. Primeramente calcularemos kP en donde k está en un intervalo pequeño. Posteriormente calcularemos lP en donde l está en un intervalo más grande de tal manera que al hacer $kP + lP = (k+l)P$, el número $(k+l)$ se encuentre en el intervalo $(p+1-2\sqrt{q}, p+1+2\sqrt{q})$.

Describiremos primero cómo hacer los llamados *Pasos-pequeños* y se mostrará como ejemplo cómo se realiza este proceso para calcular el número de puntos en nuestra curva elíptica $y^2 = x^3 - x + 188$. Calcularemos primero un número s el cual será igual a la parte entera del número raíz cuarta de q, en nuestro ejemplo será la raíz cuarta de 751.

Algoritmo	Ejemplo
$s = [\sqrt[4]{q}]$	$s = 6 = \sqrt[4]{751}$

A continuación haremos una lista con los primeros s múltiplos del punto P elegido, en nuestro ejemplo el punto P será $(1, 375)$.

Algoritmo	Ejemplo
P	$P = (1, 375)$
$2P$	$2P = (2, 378)$
$\vdots$	$3P = (6, 361)$
$\vdots$	$4P = (121, 712)$
$(s-1)P$	$5P = (57, 419)$
sP	$6P = (97, 129)$

y calcularemos los inverso aditivos de estos puntos. Estos últimos puntos, los originales y el punto en la curva nos darán una primera lista.

Algoritmo	Ejemplo
$-sP$	$-6P = (97, -129) = (97, 215)$
$-(s-1)P$	$-5P = (57, -419) = (57, 332)$
$\vdots$	$-4P = (121, -712) = (121, 39)$
$\vdots$	$-3P = (6, -361) = (6, 390)$
$-2P$	$-2P = (2, -378) = (2, 373)$
$-P$	$-P = (1, -375) = (1, 376)$
0	$0 = (\infty, \infty)$
P	$P = (1, 375)$
$2P$	$2P = (2, 378)$
$\vdots$	$3P = (6, 361)$
$\vdots$	$4P = (121, 712)$
$(s-1)P$	$5P = (57, 419)$
sP	$6P = (97, 129)$

Con este sencillo cálculo quedará concluida la etapa de *Paso-pequeño*. Antes de describir la etapa de *Paso-gigante* deberemos calcular dos puntos, Q y R los cuáles están dados por $(2s+1)P$ y $(q+1)P$, respectivamente.

Algoritmo	Ejemplo
$Q=(2s+1)P$ $R=(q+1)P$	$Q=(2*6+1)P=13P=(217,504)$ $R=(751+1)P=752P=(296,245)$

Una vez calculados estos puntos, haremos los *Pasos Gigantes*, para ello calcularemos primero un número t, el cual será la parte entera de $2\sqrt{q}/(2s+1)$ y haremos una lista que incluya a los primeros t múltiplos de Q esto es Q, $2Q$,...,tQ.

Algoritmo	Ejemplo
$t=[2\sqrt{q}/(2s+1)]$	$t=[2\sqrt{751}/13]=54{,}08/13=4$
Q $\vdots$ $\vdots$ tQ	$Q=13P=(217\ ,\ 504)$ $2Q=26P=(161\ ,\ \ 1\ )$ $3Q=39P=(270\ ,\ 589)$ $4Q=52P=(381\ ,\ \ 69\,)$

además también calcularemos los puntos $-Q,...,-tQ$

Algoritmo	Ejemplo
$-Q$ $\vdots$ $\vdots$ $-tQ$	$-Q=-13P=(217\ ,\ -504)$ $-2Q=-26P=(161\ ,\ \ -1\ )$ $-3Q=-39P=(270\ ,\ -589)$ $-4Q=-52P=(381\ ,\ \ -69\,)$

A cada uno de los múltiplos de Q que acabamos de calcular le sumaremos el punto R creando una nueva lista, además de que en está nueva lista aparecerá R mismo.

Algoritmo	Ejemplo
$R - tQ$	$R - 4Q = 752P - 52P = 700P = (205\ ,\ 161)$
$\vdots$	$R - 3Q = 752P - 39P = 713P = (734\ ,\ 552)$
$\vdots$	$R - 2Q = 752P - 26P = 726P = (\ 1\ ,\ 376)$
$R - Q$	$R - Q = 752P - 13P = 739P = (180\ ,\ 408)$
R	$R = 752P \qquad = 752P = (296\ ,\ 245)$
$R + Q$	$R + Q = 752P + 13P = 765P = (484\ ,\ 590)$
$\vdots$	$R + 2Q = 752P + 26P = 778P = (508\ ,\ 668)$
$\vdots$	$R + 3Q = 752P + 39P = 791P = (720\ ,\ 570)$
$R + tQ$	$R + 4Q = 752P + 52P = 804P = (\ 47\ ,\ 335)$

El siguiente paso será comparar los puntos de la forma jP con los puntos de la forma $R + iQ$ y ver cuales puntos de entre estas dos listas coinciden, es decir verificar para qué i y j se cumple:

$$R + iQ = jP$$

$$\begin{aligned} \text{para alguna} \quad & j \in \{0, \pm 1, \pm 2, ..., \pm s\} \\ \text{y alguna} \quad & i \in \{0, \pm 1, \pm 2, ..., \pm t\} \end{aligned}$$

pero esto ¿de que nos servirá? Debemos notar que cualquier número en el intervalo $(q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q})$, lo podemos escribir de la forma $q + 1 + i(2s + 1) - j$, para alguna $j \in \{0, \pm 1, \pm 2, ..., \pm s\}$ y alguna $i \in \{0, \pm 1, \pm 2, ..., \pm t\}$. De tal manera que

$$(q + 1 + i(2s + 1) - j)P = (q + 1)P + i(2s + 1)P - jP = R + iQ - jP.$$

por lo que al variar tanto i como j en el número $q + 1 + i(2s + 1) - j$, este variara en el intervalo $(q+1-2\sqrt{q}, q+1+2\sqrt{q})$ y cubrirá a todos los enteros en éste intervalo.

Continuando con nuestro ejemplo la lista que compara los puntos jP con los puntos $R + iQ$ está en la tabla 5, al final del capítulo, no se pone aquí dado lo extensa que es. Podemos notar que de todas las parejas de puntos que obtuvimos los únicos que son iguales son $R-2Q$ y $-P$, los cuales tienen asignado al punto $(1, 376)$, de tal manera que $R - 2Q + P = 0$, pero recordando que $Q = 13P$ y $R = 752P$ entonces $752P - 2(13)P + P = (752 - 26 + 1)P = 727P = 0$ por lo que el número m que buscamos es 727, el cual es un número primo, de lo cual podemos deducir (por la observación 3.4.7) que cualquier punto en la curva será un generador de la curva elíptica, es decir, que si tomamos 2 puntos P y Q en la curva existe $k \in \mathbb{Z}$ tal que $P = kQ$.

4.6. PROBLEMA DEL LOGARITMO DISCRETO EN CURVAS ELÍPTICAS

En la sección de criptografía vimos que algunos métodos de encriptación están basados en el problema del logaritmo discreto, ya que nuestra intención es transladar algunos de estos métodos a curvas elípticas será importante ver cómo transladar este problema a curvas elípticas.

El problema del logaritmo discreto consiste en calcular x a partir de la expresión $y \equiv a^x \pmod{p}$ en donde p es un número primo y a es una constante. Dado que el problema de multiplicar un mismo número k veces en $\mathbb{Z}_q$ tiene su análogo en la suma k veces de un punto $P \in \mathbf{E}(\mathbb{Z}_q)$ en las curvas elípticas, el problema del logaritmo discreto se verá de la siguiente forma en curvas elípticas.

Sea R una curva elíptica bajo un campo $\mathbb{F}_q$ y tomemos un punto B en $\mathbf{E}$. El problema es, dado $P \in \mathbf{E}$ encontrar un número k, tal que

$$kB = P$$

si es que este número k existe.

A primera vista el problema parecería sencillo pero recordemos que las fórmulas para la suma de dos puntos no eran fórmulas sencillas lo cual complica los calculos, mas aún cuando el campo sobre el que esta definida la curva es muy grande. A continuación veamos un método de encriptación basado en este problema.

4.7. MÉTODO ELGAMAL EN CURVAS ELÍPTICAS

Recordemos que en el método ElGamal normal elegíamos un número primo p y un número g que generará a todos los elementos de 1 a p módulo p, es decir, g tiene la propiedad de que para cualquier $s \in \mathbb{Z}$ existe un $k \in \mathbb{Z}$ tal que

$$g^k \equiv s \pmod{p},$$

y este k es precisamente lo que se tiene que encontrar.

Para pasar este método a curvas elípticas necesitaremos una curva elíptica $\mathbf{E}$ definida en un campo $\mathbb{F}_q$ y un punto $P \in \mathbf{E}(\mathbb{F}_q)$, tal que P genere a todos los puntos en la curva, esto es que para todo $Q \in \mathbf{E}(\mathbb{F}_q)$, existe $k \in \mathbb{Z}$ tal que

$$kP = Q$$

Garantizar lo anterior es un gran problema, que podemos resolver si logramos que $\#\Big(\mathbf{E}(\mathbb{F}_q)\Big)$ sea un número primo, como en el caso de nuestro ejemplo, la curva elíptica tiene 727 puntos.

Aquí necesitaremos de dos personas que deseen enviarse un texto de manera confidencial, llamemos a estas persona $\mathbf{A}$ y $\mathbf{B}$. De común acuerdo estas personas deciden de qué tamaño serán las unidades de mensaje y deciden qué punto en la curva asignaran a cada unidad de mensaje. En el caso de nuestro ejemplo diremos que las unidades de mensaje son de tamaño 1 y éstas consistirán de las 27 letras del alfabeto, donde además cada letra tendrá asignado un punto en la curva como se ejemplifico en la sección 4.2 (Ejemplo pág 95-96) y se muestra en la tabla 4.

Además de esto elegirán un punto $Z \in \mathbf{E}$, en nuestro ejemplo elegiremos el punto $(680, 94)$. Debemos notar que toda esta información es pública, es decir, cualquier persona puede tener acceso a estos datos, además de $\mathbf{A}$ y $\mathbf{B}$.

Posteriormente ambas personas deberan elegir un número entero e_i (es decir, e_A para $\mathbf{A}$ y e_B para $\mathbf{B}$) el cual mantendrán en secreto, este punto será la llave secreta de la persona respectiva. Además de esto calcularán $e_i Z$ que será su llave pública, la cual deberán enviar a la otra persona. Los

puntos en la curva que son la llave pública de cada persona (es decir e_AZ y e_BZ) también podrán ser conocidos por cualquier persona.

A continuación supondremos que **A** desea enviar una unidad de mensaje a la persona **B**, para ello buscará el punto asociado a la unidad de mensaje respectiva digamos que el punto es $P_m \in \mathbf{E}(\mathbb{F}_q)$. La persona **A** que es la que desea enviar el punto P_m, elegirá un número entero aleatorio k y calculará el punto en la curva $P_m + k(e_BZ)$. Una vez que hecho este cálculo, enviará a **B** la pareja puntos

$$\Big(kZ, P_m + k(e_BZ)\Big)$$

y es todo lo que hace **A**.

A la persona **B** le corresponde la labor de descifrar el mensaje que le mandó **A**, para ello sumará la primera coordenada de la pareja que le envió **A** consigo misma tantas veces como lo indique su clave secreta, es decir, calculara el punto $e_B(kZ)$. Una vez obtenido este punto lo restará de la segunda coordenada de la pareja que envio **A**, esto es

$$P_m + k(e_BZ) - e_B(kZ)$$

con lo cual obtendrá el valor de P_m, con lo que podrá recuperar la unidad de mensaje que deseaba enviar **A**.

Para continuar con nuestro ejemplo, según el algoritmo cada persona deberá escoger un número que será la llave secreta, elegiremos para la persona **A**: $e_A = 50$ y para **B**: $e_B = 19$, y de acuerdo al punto Z elegido anteriormente $((680, 94))$ tendremos que $e_AZ = (154, 176)$ y $e_BZ = (740, 362)$, los cuales serán las llaves públicas, por lo que **A** conoce e_BZ y **B** conoce e_AZ.

Con lo anterior procedamos a enviar las unidades de mensaje. Digamos que la persona **A** desea enviar a **B** la unidad de mensaje H, la cual, de acuerdo a la tabla 4, tiene asociado el punto $(144, 190)$, entonces supongamos que la persona **A** eligió como número k a 27 y entonces calcula kZ que es $27(680, 94) = (395, 610)$ y $k(e_BZ)$, es decir, calcula $27(740, 362)$ el cual es $(331, 367)$. Seguido de esto calcula ahora $P_m + k(e_BZ)$, de lo cual obtiene el punto $(398, 425)$. Finalmente envía a **B** la pareja

$$\Big(kZ, P_m + k(e_BZ)\Big) = \Big((395, 610), (398, 425)\Big)$$

La persona **B** recibirá $\Big((395, 610), (398, 425)\Big)$, con lo cual debe calcular cuál es la unidad de mensaje que le envió A. Para ello calculará $k(e_b Z) = 19(395, 610)$ de lo cual obtendrá $(331, 367)$, este punto se lo restará a $(398, 425)$ y el resultado será $(144, 190)$, de donde, fijandonos en la tabla 4, se puede ver que corresponde a la letra H, que es la unidad de mensaje que deseaba enviarle la persona **A**.

Aquí debemos mencionar que si una tercera persona a la que llamaremos **C** desea intercambiar información por medio de este método con la persona **A** o con **B**, bastará con que conozca cual es la curva elíptica, los puntos en la curva asociados a cada unidad de mensaje, el punto Z y las llave pública de la persona a la que desea enviarle el mensaje, con esto podra seguir el proceso y estar en posibilidad de enviar y recibir mensajes con cualquiera de las dos personas.

4.8. MÉTODO DE MASSEY-OMURA EN CURVAS ELÍPITICAS

Algoritmo

Tomemos a dos personas **A** y **B**, las cuales de común acuerdo eligen una curva elíptica **E** definida bajo un campo $\mathbb{F}_q$ y además se ponen de acuerdo en definir las unidades de mensaje, a las cuales ya les ha asignado un elemento en **E**.

Dado que ambos conocen la ecuación de **E** pueden calcular el número de puntos que tiene **E** y a este número le llaman N. Entonces cada uno elige secretamente un entero e entre 1 y N tal que $(e, N) = 1$ (es decir, e_A para **A** y e_B para **B**). Una vez elegido e cada uno calculará un número d, el cual será el inverso de e modulo N, es decir

$$d \equiv e^{-1} \pmod{N}$$

esto lo pueden hacer mediante el algoritmo de Euclides.

Después de esto comienza el proceso de encriptación del mensaje. Supongamos que **A** va a enviar el punto P_m que corresponde a una unidad de

mensaje a la persona **B**, entonces suma e_A veces el punto P_m y le envía a **B** el punto $e_A P_m$.

La persona **B** lo que recibirá será una pareja $(x, y) \in \mathbf{E}$ de la cual no podrá recuperar P_m ya que desconoce e_A y d_A, por lo que suma e_B veces el punto (x, y) y el punto resultante lo envá a **A**, es decir, A recibe $e_B e_A P_m$.

Cuando **A** recibe $e_B e_A P_m$ lo suma $d_{\mathbf{A}}$ veces para así obtener $d_{\mathbf{A}} e_{\mathbf{B}} e_{\mathbf{A}} P_m$ y envía este punto de regreso a **B**. Aquí debemos recordar que $d_{\mathbf{A}} e_{\mathbf{A}} \equiv 1 \pmod{N}$, por lo que tendremos que $d_A e_A - 1 = zN$ para algún $z \in \mathbb{N}$, de tal manera que $d_A e_A = zN + 1$. Por lo anterior tenemos que el último punto que envió A es

$$e_B e_A P_m = (zN + 1) e_B P_m = zN e_B P_m + e_m P_m$$

y como el número de puntos en **E** es N el cual es un número primo que corresponde al orden de la curva **E**, entonces $NP = 0$, para toda $P \in \mathbf{E}$. De tal manera que **A** realmente envió

$$zN e_B P_m + e_m P_m = N(z e_B P_m) + e_B P_m = 0 + e_B P_m = e_B P_m$$

por lo que **B** recibió $e_B P_m$. Entonces **B** suma d_B veces el último punto que envió **B** obteniendo $d_B d_a e_B e_A P_m = d_B e_B P_m$, lo cual se simplifica en P_m que es lo que **A** le quería hacer llegar. Dado que **B** ya conoce P_m, entonces puede recuperar la unidad de mensaje asociada a este punto, con lo cual terminamos la descripción del método.

Personas distintas de A y B que quisieran encontrar P_m lo único que sabrían sería $e_A P_m$, $e_B e_A P_m$ y $e_B P_m$. Tratar de encontrar P_m a partir de estos tres datos conduce a resolver el problema del logaritmo discreto en curvas elípticas, ya que sería la única manera de encontrar e_B a partir de $e_A P_m$ y $e_B e_A P_m$. Si alguna persona distinta de **A** o **B** se encuentra e_B, entonces puede calcular d_B y entonces puede encontrar $d_B(e_B P_m) = P_m$, pero como el problema del logaritmo discreto en curvas sólo se puede resolver en tiempo exponencial, este método es bastante seguro.

Ejemplo

Para mostrar cómo se desarrolla este ejemplo, utilizaremos nuestra curva elíptica de ejemplo ($y^2 = x^3 - x + 188$), las unidades de mensaje utilizadas antes y los puntos asociados a estas unidades como en la tabla 4.

En nuestro ejemplo la persona **A** escogió el número $e_A = 45$ el cual tiene como inverso multiplicativo módulo 727 a $d_A = 517$, y la persona **B** eligió $e_B = 117$ que tiene como inverso multiplicativo a $d_B = 87$.

Si la persona **A** desea enviarle a **B** la unidad de mensaje Z que tiene asociado el punto (520,328) de la curva **E** (el cual corresponde al punto P_m en el algoritmo), entonces deberá calcular $45(520, 328)$ (correspondiente a $e_A P_m$), lo cual le dará como resultado $(649, 694)$ y este punto en la curva será el que mandará a **B**.

La persona **B** al recibir este punto calcula $117(649, 694)$ que le arroja como resultado $(187, 701)$ (de acuerdo al algoritmo este punto es $e_B e_a P_m$) y se lo envía de regreso a **A**.

A una vez que recibe $(187, 701)$ sumará este punto 517 veces para obtener el punto $(92, 606)$ y enviará este punto a **B**. La persona **B** al recibir este punto sabe que de acuerdo al algoritmo corresponde al punto $d_A e_B e_A$ por lo que calcula $87(92, 606)$, lo cual le deberá dar como resultado el punto que la persona **A** le deseaba enviar, es decir $(520, 328)$, que buscando en la tabla 4, puede ver que corresponde a la letra Z. Por lo que finalmente recibe el mensaje que deseaba enviarle **A**.

Sobre estos métodos debemos mencionar que no son la única manera en los que se puede aplicar, podemos hacer variaciones sobre los mismos. Por ejemplo, podemos aumentar la longitud de las unidades de mensaje, es decir, en lugar de tomar unidades de longitud uno, hacerlas de longitud 2, 3 o mayores. También podemos introducir "basura" en el texto. En este caso, si tenemos la palabra MENSAJE, podemos cambiarle por la palabra MENSWAJE y posteriormente hacer la encriptación, es decir, separar el texto en unidades de mensaje y cada determinado intervalo introducir una letra cualquiera en el texto. En fin se pueden hacer muchas modificaciones que dependen de la imaginación de la persona que haga el sistema de encriptación. Todo esto con el fin de complicarle el trabajo al criptoanalista y hacerle complicado su trabajo.

Con esto finalizamos este trabajo. Debemos mencionar que existen varios problemas abiertos sobre los distintos temas que se han presentado en este trabajo. En principio uno de los problemas a los que se enfrenta la criptografía actual son las investigaciones que se hacen para desarrollar una

computadora de tipo cuántica, la cual podría reducir considerablemente el tiempo de algunos procesos. Entre los procesos que se podrían hacer mas eficientemente están los problemas del logaritmo discreto y el de la factorización en primos de un número cualquiera, que son los problemas en los que están basados algunos de los métodos que hemos revisado. Aunque cabe destacar que al no existir un algoritmo que no sea de tiempo exponencial para su resolución, lo que sucederá es que se utilizarán números de un mucho mayor número de cifras que los empleados actualmente.

Por otro lado debemos mencionar que en el número 32 del Scientific American Latinoamerica se presenta un muy interesante artículo sobre CRIPTOGRAFÍA CUÁNTICA, lo cual es un salto muy importante en la criptografía ya que es posible determinar cuándo alguna persona ha intentado interceptar el mensaje, pues esto introduce errores en los mensajes, de lo cual se pueden percatar los emisores. Además de lo anterior se cree que la criptografía de tipo cuántica seguirá siendo segura a pesar de contar con ordenadores cuánticos. De hecho algunas empresas en el 2003 presentaron productos que utilizan esta reciente tecnología.

En el caso de las curvas elípticas tenemos algunos problemas sin resolver, de los cuales revisamos algunos en la tesis, como lo son el calcular el número de puntos que hay en una curva elíptica y el problema del logaritmo discreto en curvas elípticas de manera que los algoritmos no sean de tiempo exponencial. En el caso del problema del número de puntos en una curva elíptica existe una demostración realizada por René Schoof llamado Algoritmo de Schoof, el cual desafortunadamente es un algoritmo de tiempo exponencial.

Otro de los problemas para los cuales se han utilizado las curvas elípticas es para encontrar la factorización de un número entero, método realizado por H. W. Lenstra. El interés de muchos criptografos y criptoanalistas en las curvas elípticas se debe en parte a éste método, el cual, en muchos sentidos es mejor que los que se conocían anteriormente para encontrar la factorización de un número entero, aunque la mejora no es lo suficientemente significativa para convertirse en un peligro para los criptosistemas cuya seguridad está basada en la dificultad de encontrar la factorización de un número entero.

La factorización de un número entero en curvas elíptica es un problema el cual me hubiera gustado abordar en esta tesis, pero desde mi punto de

vista lo desarrollado aquí tanto en criptografía como en curvas elípticas es un buen acercamiento con estos temas para un estudiante de licenciatura, para los cuales espero pueda servir como material de apoyo.

Tabla 1

x	$x^3 - x$ +188
1	188
5	308
9	157
13	119
17	578
21	416
25	17
29	516
33	44
37	487
41	727
45	397
49	632
53	314
57	578
61	306
65	633
69	441
73	114
77	36
81	591
85	661
89	630
93	131
97	299
101	16
105	417
109	384
113	301
117	552
121	19
125	588
129	390

x	$x^3 - x$ +188
2	194
6	398
10	427
14	665
18	745
22	300
26	465
30	122
34	406
38	199
42	636
46	599
50	472
54	639
58	733
62	387
66	736
70	662
74	549
78	30
82	240
86	61
90	628
94	72
98	279
102	131
106	12
110	306
114	646
118	665
122	747
126	525
130	383

x	$x^3 - x$ +188
3	212
7	524
11	6
15	544
19	269
23	316
27	318
31	659
35	221
39	139
43	46
47	326
51	612
55	537
59	485
63	89
67	484
71	552
75	677
79	492
83	381
87	728
91	415
95	577
99	96
103	107
107	243
111	137
115	173
119	735
123	705
127	467
131	405

x	$x^3 - x$ +188
4	248
8	692
12	402
16	513
20	658
24	470
28	333
32	631
36	246
40	313
44	465
48	335
52	307
56	14
60	591
64	169
68	634
72	117
76	504
80	677
84	269
88	415
92	748
96	150
100	507
104	701
108	365
112	634
116	390
120	17
124	650
128	420
132	462

x	$x^3 - x$ +188
133	560
137	731
141	536
145	359
149	584
153	93
157	21
161	1
165	417
169	151
173	338
177	611
181	603
185	698
189	529
193	480
197	184
201	25
205	387
209	152
213	455
217	178
221	456
225	171
229	458
233	199
237	529
241	330
245	737
249	632
253	399
257	422
261	334
265	519
269	610
273	240
277	544
281	404
285	204

x	$x^3 - x$ +188
134	705
138	373
142	522
146	34
150	44
154	185
158	90
162	143
166	728
170	727
174	524
178	503
182	297
186	290
190	115
194	156
198	46
202	169
206	158
210	397
214	519
218	157
222	446
226	268
230	7
234	47
238	21
242	313
246	556
250	383
254	178
258	325
262	457
266	207
270	710
274	97
278	254
282	63
286	659

x	$x^3 - x$ +188
135	152
139	92
143	609
147	585
151	404
155	450
159	356
163	506
167	533
171	70
175	252
179	712
183	332
187	247
191	90
195	245
199	345
203	23
207	414
211	400
215	365
219	693
223	266
227	219
231	185
235	548
239	190
243	246
247	349
251	132
255	730
259	274
263	650
267	740
271	177
275	96
279	130
283	663
287	577

x	$x^3 - x$ +188
136	409
140	645
144	52
148	516
152	168
156	143
160	74
164	345
168	589
172	439
176	279
180	493
184	714
188	575
192	460
196	2
200	336
204	344
208	410
212	167
216	750
220	290
224	673
228	30
232	247
236	206
240	291
244	135
248	122
252	636
256	559
260	275
264	168
268	622
272	519
276	243
280	178
284	708
288	715

x	$x^3 - x$ +188
289	328
293	409
297	80
301	476
305	479
309	473
313	91
317	468
321	486
325	529
329	230
333	724
337	142
341	370
345	290
349	286
353	742
357	540
361	64
365	449
369	577
373	81
377	96
381	255
385	191
389	288
393	179
397	248
401	128
405	203
409	106
413	221
417	181
421	370
425	421
429	718
433	143
437	582
441	166

x	$x^3 - x$ +188
290	173
294	491
298	495
302	569
306	346
310	210
314	545
318	233
322	409
326	706
330	6
334	195
338	155
342	270
346	173
350	248
354	128
358	197
362	88
366	185
370	121
374	280
378	295
382	550
386	678
390	312
394	587
398	385
402	90
406	86
410	6
414	234
418	403
422	146
426	598
430	641
434	659
438	285
442	654

x	$x^3 - x$ +188
291	256
295	84
299	445
303	221
307	547
311	305
315	630
319	404
323	11
327	586
331	260
335	168
339	694
343	720
347	630
351	57
355	136
359	500
363	31
367	615
371	383
375	470
379	509
383	133
387	477
391	423
395	355
399	657
403	211
407	152
411	113
415	478
419	129
423	201
427	327
431	140
435	24
439	363
443	39

x	$x^3 - x$ +188
292	583
296	696
300	687
304	189
308	337
312	13
316	352
320	236
324	49
328	175
332	247
336	649
340	263
344	224
348	165
352	470
356	21
360	704
364	650
368	243
372	618
376	657
380	744
384	512
388	345
392	627
396	240
400	319
404	497
408	407
412	433
416	208
420	116
424	541
428	365
432	723
436	497
440	71
444	580

x	$x^3 - x$ +188
445	30
449	558
453	632
457	636
461	203
465	468
469	313
473	122
477	279
481	417
485	169
489	670
493	51
497	198
501	744
505	571
509	63
513	355
517	329
521	369
525	108
529	681
533	219
537	608
541	730
545	218
549	207
553	330
557	220
561	261
565	86
569	79
573	624
577	603
581	400
585	399
589	233
593	286
597	191

x	$x^3 - x$ +188
446	648
450	651
454	296
458	718
462	48
466	172
470	723
474	583
478	136
482	517
486	608
490	42
494	705
498	728
502	495
506	390
510	46
514	598
518	177
522	669
526	205
530	671
534	198
538	672
542	224
546	740
550	351
554	192
558	647
562	598
566	429
570	524
574	516
578	38
582	225
586	710
590	375
594	355
598	283

x	$x^3 - x$ +188
447	187
451	440
455	431
459	544
463	412
467	419
471	198
475	133
479	608
483	505
487	208
491	101
495	568
499	491
503	254
507	241
511	85
515	170
519	129
523	346
527	454
531	86
535	377
539	209
543	717
547	32
551	40
555	374
559	667
563	552
567	413
571	634
575	97
579	688
583	538
587	31
591	302
595	233
599	208

x	$x^3 - x$ +188
448	155
452	682
456	292
460	120
464	550
468	464
472	246
476	280
480	199
484	387
488	477
492	102
496	397
500	244
504	27
508	130
512	186
516	579
520	191
524	157
528	110
532	434
536	11
540	727
544	713
548	353
552	31
556	131
560	286
564	129
568	44
572	415
576	124
580	306
584	594
588	621
592	20
596	677
600	723

x	$x^3 - x$ +188
601	332
605	342
609	605
613	3
617	422
621	744
625	602
629	380
633	462
637	481
641	70
645	364
649	245
653	97
657	304
661	499
665	315
669	136
673	346
677	578
681	465
685	391
689	740
693	394
697	488
701	655
705	528
709	491
713	177
717	721
721	254
725	662
729	76
733	382
737	462
741	700
745	729
749	182

x	$x^3 - x$ +188
602	543
606	17
610	591
614	396
618	567
622	737
626	539
630	357
634	575
638	75
642	743
646	710
650	360
654	77
658	245
662	497
666	466
670	536
674	340
678	262
682	686
686	494
690	70
694	549
698	62
702	495
706	730
710	400
714	640
718	332
722	611
726	359
730	711
734	549
738	257
742	219
746	68
750	188

x	$x^3 - x$ +188
603	611
607	324
611	482
615	718
619	665
623	707
627	477
631	359
635	737
639	493
643	11
647	426
651	620
655	226
659	379
663	712
667	107
671	450
675	623
679	259
683	493
687	207
691	536
695	362
699	69
703	41
707	662
711	63
715	130
719	496
723	43
727	657
731	469
735	614
739	725
743	435
747	128
0	188

x	$x^3 - x$ +188
604	542
608	518
612	284
616	224
620	722
624	660
628	422
632	392
636	203
640	239
644	133
648	269
652	280
656	550
660	712
664	399
668	746
672	635
676	450
680	575
684	643
688	287
692	642
696	590
700	515
704	50
708	330
712	237
716	155
720	468
724	58
728	60
732	107
736	583
740	370
744	603
748	164

Tabla 2

y	y^2
1	1
5	25
9	81
13	169
17	289
21	441
25	625
29	90
33	338
37	618
41	179
45	523
49	148
53	556
57	245
61	717
65	470
69	255
73	72
77	672
81	553
85	466
89	411
93	388
97	397
101	438
105	511
109	616
113	2
117	171
121	372
125	605
129	119
133	416

y	y^2
2	4
6	36
10	100
14	196
18	324
22	484
26	676
30	149
34	405
38	693
42	262
46	614
50	247
54	663
58	360
62	89
66	601
70	394
74	219
78	76
82	716
86	637
90	590
94	575
98	592
102	641
106	722
110	84
114	229
118	406
122	615
126	105
130	378
134	683

y	y^2
3	9
7	49
11	121
15	225
19	361
23	529
27	729
31	210
35	474
39	19
43	347
47	707
51	348
55	21
59	477
63	214
67	734
71	535
75	368
79	233
83	130
87	59
91	20
95	13
99	38
103	95
107	184
111	305
115	458
119	643
123	109
127	358
131	639
135	201

y	y^2
4	16
8	64
12	144
16	256
20	400
24	576
28	33
32	273
36	545
40	98
44	434
48	51
52	451
56	132
60	596
64	341
68	118
72	678
76	519
80	392
84	297
88	234
92	203
96	204
100	237
104	302
108	399
112	528
116	689
120	131
124	356
128	613
132	151
136	472

y	y^2
137	745
141	355
145	748
149	422
153	128
157	617
161	387
165	189
169	23
173	640
177	538
181	468
185	430
189	424
193	450
197	508
201	598
205	720
209	123
213	309
217	527
221	26
225	308
229	622
233	217
237	595
241	254
245	696
249	419
253	174
257	712
261	531
265	382
269	265
273	180
277	127
281	106
285	117

y	y^2
138	269
142	638
146	288
150	721
154	435
158	181
162	710
166	520
170	362
174	236
178	142
182	80
186	50
190	52
194	86
198	152
202	250
206	380
210	542
214	736
218	211
222	469
226	8
230	330
234	684
238	319
242	737
246	436
250	167
254	681
258	476
262	303
266	162
270	53
274	727
278	682
282	669
286	688

y	y^2
139	546
143	172
147	581
151	271
155	744
159	498
163	284
167	102
171	703
175	585
179	499
183	445
187	423
191	433
195	475
199	549
203	655
207	42
211	212
215	414
219	648
223	163
227	461
231	40
235	402
239	45
243	471
247	178
251	668
255	439
259	242
263	77
267	695
271	594
275	525
279	488
283	483
287	510

y	y^2
140	74
144	459
148	125
152	574
156	304
160	66
164	611
168	437
172	295
176	185
180	107
184	61
188	47
192	65
196	115
200	197
204	311
208	457
212	635
216	94
220	336
224	610
228	165
232	503
236	122
240	524
244	207
248	673
252	420
256	199
260	10
264	604
268	479
272	386
276	325
280	296
284	299
288	334

y	y^2
289	160
293	235
297	342
301	481
305	652
309	104
313	339
317	606
321	154
325	485
329	97
333	492
337	168
341	627
345	367
349	139
353	694
357	530
361	398
365	298
369	230
373	194
377	190
381	218
385	278
389	370
393	494
397	650
401	87
405	307
409	559
413	92
417	408
421	5
425	385
429	46
433	490
437	215
441	723

y	y^2
290	739
294	71
298	186
302	333
306	512
310	723
314	215
318	490
322	46
326	385
330	5
334	408
338	92
342	559
346	307
350	87
354	650
358	494
362	370
366	278
370	218
374	190
378	194
382	230
386	298
390	398
394	530
398	694
402	139
406	367
410	627
414	168
418	492
422	97
426	485
430	154
434	606
438	339
442	104

y	y^2
291	569
295	660
299	32
303	187
307	374
311	593
315	93
319	376
323	691
327	287
331	666
335	326
339	18
343	493
347	249
351	37
355	608
359	460
363	344
367	260
371	208
375	188
379	200
383	244
387	320
391	428
395	568
399	740
403	193
407	429
411	697
415	246
419	578
423	191
427	587
431	264
435	724
439	465
443	238

y	y^2
292	401
296	500
300	631
304	43
308	238
312	465
316	724
320	264
324	587
328	191
332	578
336	246
340	697
344	429
348	193
352	740
356	568
360	428
364	320
368	244
372	200
376	188
380	208
384	260
388	344
392	460
396	608
400	37
404	249
408	493
412	18
416	326
420	666
424	287
428	691
432	376
436	93
440	593
444	374

$\mathbb{F}_{751}$	
y	y^2
445	512
449	333
453	186
457	71
461	739
465	688
469	669
473	682
477	727
481	53
485	162
489	303
493	476
497	681
501	167
505	436
09	737
513	319
517	684
521	330
525	8
529	469
533	211
537	736
541	542
545	380
549	250
553	152
557	86
561	52
565	50
569	80
573	142
577	236
581	362
585	520
589	710
593	181

$\mathbb{F}_{751}$	
y	y^2
446	652
450	481
454	342
458	235
462	160
466	117
470	106
474	127
478	180
482	265
486	382
490	531
494	712
498	174
502	419
506	696
510	254
514	595
518	217
522	622
526	308
530	26
534	527
538	309
542	123
546	720
550	598
554	508
558	450
562	424
566	430
570	468
574	538
578	640
582	23
586	189
590	387
594	617

$\mathbb{F}_{751}$	
y	y^2
447	43
451	631
455	500
459	401
463	334
467	299
471	296
475	325
479	386
483	479
487	604
491	10
495	199
499	420
503	673
507	207
511	524
515	122
519	503
523	165
527	610
531	336
535	94
539	635
543	457
547	311
551	197
555	115
559	65
563	47
567	61
571	107
575	185
579	295
583	437
587	611
591	66
595	304

$\mathbb{F}_{751}$	
y	y^2
448	187
452	32
456	660
460	569
464	510
468	483
472	488
476	525
480	594
484	695
488	77
492	242
496	439
500	668
504	178
508	471
512	45
516	402
520	40
524	461
528	163
532	648
536	414
540	212
544	42
548	655
552	549
556	475
560	433
564	423
568	445
572	499
576	585
580	703
584	102
588	284
592	498
596	744

y	y^2
597	435
601	721
605	288
609	638
613	269
617	683
621	378
625	105
629	615
633	406
637	229
641	84
645	722
649	641
653	592
657	575
661	590
665	637
669	716
673	76
677	219
681	394
685	601
689	89
693	360
697	663
701	247
705	614
709	262
713	693
717	405
721	149
725	676
729	484
733	324
737	196
741	100
745	36
749	4

y	y^2
598	128
602	422
606	748
610	355
614	745
618	416
622	119
626	605
630	372
634	171
638	2
642	616
646	511
650	438
654	397
658	388
662	411
666	466
670	553
674	672
678	72
682	255
686	470
690	717
694	245
698	556
702	148
706	523
710	179
714	618
718	338
722	90
726	625
730	441
734	289
738	169
742	81
746	25
750	1

y	y^2
599	574
603	125
607	459
611	74
615	472
619	151
623	613
627	356
631	131
635	689
639	528
643	399
647	302
651	237
655	204
659	203
663	234
667	297
671	392
675	519
679	678
683	118
687	341
691	596
695	132
699	451
703	51
707	434
711	98
715	545
719	273
723	33
727	576
731	400
735	256
739	144
743	64
747	16
0	0

y	y^2
600	271
604	581
608	172
612	546
616	201
620	639
624	358
628	109
632	643
636	458
640	305
644	184
648	95
652	38
656	13
660	20
664	59
668	130
672	233
676	368
680	535
684	734
688	214
692	477
696	21
700	348
704	707
708	347
712	19
716	474
720	210
724	729
728	529
732	361
736	225
740	121
744	49
748	9

Tabla 3

#	x	y
1	1	375
4	2	378
7	5	225
10	6	390
13	12	235
16	13	622
19	18	137
22	19	613
25	24	65
28	26	439
31	30	236
34	32	451
37	36	336
40	38	495
43	41	274
46	43	429
49	45	97
52	47	416
55	52	346
58	54	620
61	59	325
64	62	590
67	64	13
70	66	537
73	69	21
76	72	466
79	77	6
82	79	418
85	86	184
88	92	606
91	94	73
94	97	467
97	102	120
100	103	571

#	x	y
2	1	376
5	3	211
8	5	526
11	7	240
14	12	516
17	17	332
20	18	614
23	21	133
26	24	686
29	28	302
32	30	515
35	34	118
38	36	415
41	39	349
44	41	477
47	44	312
50	45	654
53	50	136
56	52	405
59	57	332
62	59	426
65	63	62
68	64	738
71	67	22
74	69	730
77	74	199
80	77	745
83	84	138
86	86	567
89	93	120
92	94	678
95	101	4
98	102	631
101	121	39

#	x	y
3	2	373
6	3	540
9	6	361
12	7	511
15	13	129
18	17	419
21	19	138
24	21	618
27	26	312
30	28	449
33	32	300
36	34	633
39	38	256
42	39	402
45	43	322
48	44	439
51	47	335
54	50	615
57	54	131
60	57	419
63	62	161
66	63	689
69	66	214
72	67	729
75	72	285
78	74	552
81	79	333
84	84	613
87	92	145
90	93	631
93	97	284
96	101	747
99	103	180
102	121	712

#	x	y
103	124	354
106	126	476
109	131	34
112	135	553
115	144	190
118	147	576
121	153	315
124	154	575
127	157	55
130	158	722
133	160	140
136	161	750
139	170	274
142	172	496
145	174	240
148	177	587
151	179	257
154	180	408
157	187	50
160	188	657
163	190	196
166	191	722
169	195	57
172	196	638
175	198	322
178	200	531
181	202	13
184	203	582
187	205	161
190	207	536
193	210	97
196	211	731
199	214	76
202	217	504
205	224	248
208	225	634
211	229	115
214	231	575
217	233	256

#	x	y
104	124	397
107	128	252
110	131	717
113	139	338
116	144	561
119	152	337
122	153	436
125	155	193
128	157	696
131	159	124
134	160	611
137	169	132
140	170	477
143	173	33
146	174	511
149	178	232
152	179	494
155	182	84
158	187	701
161	189	23
164	190	555
167	192	359
170	195	694
173	197	107
176	198	429
179	201	5
182	202	738
185	204	363
188	205	590
191	209	198
194	210	654
197	212	250
200	214	675
203	219	38
206	224	503
209	227	74
212	229	636
215	232	50
218	233	495

#	x	y
105	126	275
108	128	499
111	135	198
114	139	413
117	147	175
120	152	414
123	154	176
126	155	558
129	158	29
132	159	627
135	161	1
138	169	619
141	172	255
144	173	718
147	177	164
150	178	519
153	180	343
156	182	667
159	188	94
162	189	728
165	191	29
168	192	392
171	196	113
174	197	644
177	200	220
180	201	746
183	203	169
186	204	388
189	207	215
192	209	553
195	211	20
198	212	501
201	217	247
204	219	713
207	225	117
210	227	677
213	231	176
216	232	701
219	234	188

#	x	y
220	234	563
223	238	55
226	239	377
229	243	336
232	245	509
235	248	236
238	251	695
241	254	247
244	256	409
247	258	276
250	261	463
253	263	354
256	264	414
259	266	244
262	267	399
265	269	224
268	270	589
271	274	329
274	278	510
277	280	247
280	283	697
283	291	16
286	295	641
289	297	182
292	299	568
295	302	291
298	304	586
301	310	31
304	311	640
307	314	36
310	317	570
313	320	174
316	324	744
319	329	369
322	331	384
325	333	316
328	335	414
331	339	353
334	341	389

#	x	y
221	237	23
224	238	696
227	241	230
230	243	415
233	246	53
236	248	515
239	253	108
242	254	504
245	257	149
248	258	475
251	262	208
254	263	397
257	265	76
260	266	507
263	268	229
266	269	527
269	272	76
272	274	422
275	279	83
278	280	504
281	285	96
284	291	735
287	296	245
290	297	569
293	301	258
296	302	460
299	305	268
302	310	720
305	312	95
308	314	715
311	318	79
314	320	577
317	325	23
320	329	382
323	332	50
326	333	435
329	337	178
332	339	398
335	343	205

#	x	y
222	237	728
225	239	374
228	241	521
231	245	242
234	246	698
237	251	56
240	253	643
243	256	342
246	257	602
249	261	288
252	262	543
255	264	337
258	265	675
261	267	352
264	268	522
267	270	162
270	272	675
273	278	241
276	279	668
279	283	54
282	285	655
285	295	110
288	296	506
291	299	183
294	301	493
297	304	165
300	305	483
303	311	111
306	312	656
309	317	181
312	318	672
315	324	7
318	325	728
321	331	367
324	332	701
327	335	337
330	337	573
333	341	362
336	343	546

#	x	y
337	348	228
340	352	686
343	356	55
346	358	551
349	361	8
352	364	397
355	367	122
358	370	740
361	373	9
364	375	686
367	380	155
370	381	682
373	385	328
376	386	679
379	389	146
382	391	564
385	393	41
388	394	427
391	398	326
394	400	513
397	402	29
400	403	533
403	406	194
406	407	553
409	412	191
412	414	663
415	417	158
418	421	389
421	426	201
424	430	649
427	440	294
430	446	532
433	452	278
436	454	471
439	465	181
442	466	608
445	470	310
448	472	415
451	479	355

#	x	y
338	348	523
341	354	153
344	356	696
347	359	296
350	361	743
353	366	176
356	367	629
359	372	37
362	373	742
365	378	172
368	380	596
371	384	306
374	385	423
377	387	59
380	389	605
383	392	341
386	393	710
389	395	141
392	398	425
395	401	153
398	402	722
401	405	92
404	406	557
407	409	281
410	412	560
413	416	371
416	417	593
419	423	135
422	426	550
425	432	310
428	440	457
431	447	303
434	452	473
437	461	92
440	465	570
443	467	249
446	470	441
449	473	236
452	479	396

#	x	y
339	352	65
342	354	598
345	358	200
348	359	455
351	364	354
354	366	575
357	370	11
360	372	714
363	375	65
366	378	579
369	381	69
372	384	445
375	386	72
378	387	692
381	391	187
384	392	410
387	394	324
390	395	610
393	400	238
396	401	598
399	403	218
402	405	659
405	407	198
408	409	470
411	414	88
414	416	380
417	421	362
420	423	616
423	430	102
426	432	441
429	446	219
432	447	448
435	454	280
438	461	659
441	466	143
444	467	502
447	472	336
450	473	515
453	480	256

#	x	y
454	480	495
457	485	13
460	486	396
463	488	59
466	490	544
469	493	48
472	495	395
475	500	368
478	501	596
481	508	83
484	510	429
487	513	141
490	514	550
493	522	282
496	529	497
499	532	44
502	533	677
505	538	77
508	540	477
511	545	370
514	546	399
517	549	244
520	551	520
523	555	307
526	556	631
529	565	194
532	566	407
535	575	329
538	578	652
541	581	20
544	582	736
547	584	271
550	585	643
553	589	79
556	591	647
559	594	141
562	595	672
565	599	371
568	600	441

#	x	y
455	484	161
458	485	738
461	487	371
464	488	692
467	492	167
470	493	703
473	496	97
476	500	383
479	503	241
482	508	668
485	512	298
488	513	610
491	520	328
494	522	469
497	531	194
500	532	707
503	537	355
506	538	674
509	543	61
512	545	381
515	547	299
518	549	507
521	553	230
524	555	444
527	562	201
530	565	557
533	570	240
536	575	422
539	579	286
542	581	731
545	583	177
548	584	480
551	586	162
554	589	672
557	592	91
560	594	610
563	597	328
566	599	380
569	603	164

#	x	y
456	484	590
459	486	355
462	487	380
465	490	207
468	492	584
471	495	356
474	496	654
477	501	155
480	503	510
483	510	322
486	512	453
489	514	201
492	520	423
495	529	254
498	531	557
501	533	74
504	537	396
507	540	274
510	543	690
513	546	352
516	547	452
519	551	231
522	553	521
525	556	120
528	562	550
531	566	344
534	570	511
537	578	99
540	579	465
543	582	15
546	583	574
549	585	108
552	586	589
555	591	104
558	592	660
561	595	79
564	597	423
567	600	310
570	603	587

#	x	y
571	604	210
574	605	454
577	609	125
580	612	588
583	620	106
586	621	596
589	623	47
592	624	456
595	628	149
598	629	545
601	634	94
604	635	509
607	637	301
610	639	408
613	648	138
616	649	694
619	653	329
622	654	488
625	658	57
628	660	494
631	663	257
634	664	643
637	667	180
640	671	558
643	676	193
646	677	419
649	680	94
652	681	439
655	684	119
658	686	393
661	688	327
664	689	399
667	694	199
670	695	581
673	697	279
676	701	548
679	705	112
682	708	521

#	x	y
572	604	541
575	607	18
578	609	626
581	617	149
584	620	645
587	622	242
590	623	704
593	627	59
596	628	602
599	632	80
602	634	657
605	636	92
608	637	450
611	646	162
614	648	613
617	650	58
620	653	422
623	657	156
626	658	694
629	661	179
632	663	494
635	666	85
638	667	571
641	672	212
644	676	558
647	678	42
650	680	657
653	683	343
656	684	632
659	687	244
662	688	424
665	693	70
668	694	552
671	696	90
674	697	472
677	704	186
680	705	639
683	710	20

#	x	y
573	605	297
576	607	733
579	612	163
582	617	602
585	621	155
588	622	509
591	624	295
594	627	692
597	629	206
600	632	671
603	635	242
606	636	659
609	639	343
612	646	589
615	649	57
618	650	693
621	654	263
624	657	595
627	660	257
630	661	572
633	664	108
636	666	666
639	671	193
642	672	539
645	677	332
648	678	709
651	681	312
654	683	408
657	686	358
660	687	507
663	689	352
666	693	681
669	695	170
672	696	661
675	701	203
678	704	565
681	708	230
684	710	731

#	x	y
685	712	100
688	714	578
691	717	150
694	720	570
697	722	164
700	723	447
703	731	222
706	732	571
709	734	199
712	735	705
715	742	74
718	743	597
721	747	153
724	750	376
727	∞	∞

#	x	y
686	712	651
689	715	83
692	717	601
695	721	241
698	722	587
701	729	78
704	731	529
707	733	265
710	734	552
713	740	362
716	742	677
719	745	27
722	747	598
725	751	375

#	x	y
687	714	173
690	715	668
693	720	181
696	721	510
699	723	304
702	729	673
705	732	180
708	733	486
711	735	46
714	740	389
717	743	154
720	745	724
723	750	375
726	751	376

Tabla 4

Unidad de mensaje	Punto en **E**
A	(0,375)
C	(41,274)
E	(84,138)
G	(121,39)
I	(160,140)
K	(200,220)
M	(241,230)
Ñ	(280,247)
P	(320,174)
R	(361,8)
T	(400,238)
V	(440,294)
X	(480,256)
Z	(520,328)

Unidad de mensaje	Punto en **E**
B	(21,133)
D	(62,161)
F	(101,4)
H	(144,190)
J	(180,343)
L	(224,248)
N	(261,288)
O	(301,258)
Q	(341,362)
S	(380,155)
U	(421,362)
W	(461,92)
Y	(500,368)

Tabla 5

$R-4Q$	$700P=(205\ ,\ 161)$	$\neq$	$(\ 97\ ,\ 215)$	$-6P$
$R-4Q$	$700P=(205\ ,\ 161)$	$\neq$	$(\ 57\ ,\ 332)$	$-5P$
$R-4Q$	$700P=(205\ ,\ 161)$	$\neq$	$(121\ ,\ 39)$	$-4P$
$R-4Q$	$700P=(205\ ,\ 161)$	$\neq$	$(\ 6\ \ ,\ 390)$	$-3P$
$R-4Q$	$700P=(205\ ,\ 161)$	$\neq$	$(\ 2\ \ ,\ 373)$	$-2P$
$R-4Q$	$700P=(205\ ,\ 161)$	$\neq$	$(\ 1\ \ ,\ 376)$	$-P$
$R-4Q$	$700P=(205\ ,\ 161)$	$\neq$	$(\ \infty\ \ ,\ \infty)$	0
$R-4Q$	$700P=(205\ ,\ 161)$	$\neq$	$(\ 1\ \ ,\ 375)$	P
$R-4Q$	$700P=(205\ ,\ 161)$	$\neq$	$(\ 2\ \ ,\ 378)$	$2P$
$R-4Q$	$700P=(205\ ,\ 161)$	$\neq$	$(\ 6\ \ ,\ 361)$	$3P$
$R-4Q$	$700P=(205\ ,\ 161)$	$\neq$	$(121\ ,\ 712)$	$4P$
$R-4Q$	$700P=(205\ ,\ 161)$	$\neq$	$(\ 57\ ,\ 419)$	$5P$
$R-4Q$	$700P=(205\ ,\ 161)$	$\neq$	$(\ 97\ ,\ 129)$	$6P$

$R-3Q$	$713P=(734\ ,\ 552)$	$\neq$	$(\ 97\ ,\ 215)$	$-6P$
$R-3Q$	$713P=(734\ ,\ 552)$	$\neq$	$(\ 57\ ,\ 332)$	$-5P$
$R-3Q$	$713P=(734\ ,\ 552)$	$\neq$	$(121\ ,\ 39)$	$-4P$
$R-3Q$	$713P=(734\ ,\ 552)$	$\neq$	$(\ 6\ \ ,\ 390)$	$-3P$
$R-3Q$	$713P=(734\ ,\ 552)$	$\neq$	$(\ 2\ \ ,\ 373)$	$-2P$
$R-3Q$	$713P=(734\ ,\ 552)$	$\neq$	$(\ 1\ \ ,\ 376)$	$-P$
$R-3Q$	$713P=(734\ ,\ 552)$	$\neq$	$(\ \infty\ \ ,\ \infty)$	0
$R-3Q$	$713P=(734\ ,\ 552)$	$\neq$	$(\ 1\ \ ,\ 375)$	P
$R-3Q$	$713P=(734\ ,\ 552)$	$\neq$	$(\ 2\ \ ,\ 378)$	$2P$
$R-3Q$	$713P=(734\ ,\ 552)$	$\neq$	$(\ 6\ \ ,\ 361)$	$3P$
$R-3Q$	$713P=(734\ ,\ 552)$	$\neq$	$(121\ ,\ 712)$	$4P$
$R-3Q$	$713P=(734\ ,\ 552)$	$\neq$	$(\ 57\ ,\ 419)$	$5P$
$R-3Q$	$713P=(734\ ,\ 552)$	$\neq$	$(\ 97\ ,\ 129)$	$6P$

$R-2Q$	$726P = (\ 1\ ,\ 376)$	$\neq$	$(\ 97\ ,\ 215)$	$-6P$
$R-2Q$	$726P = (\ 1\ ,\ 376)$	$\neq$	$(\ 57\ ,\ 332)$	$-5P$
$R-2Q$	$726P = (\ 1\ ,\ 376)$	$\neq$	$(121\ ,\ 39)$	$-4P$
$R-2Q$	$726P = (\ 1\ ,\ 376)$	$\neq$	$(\ 6\ \ ,\ 390)$	$-3P$
$R-2Q$	$726P = (\ 1\ ,\ 376)$	$\neq$	$(\ 2\ \ ,\ 373)$	$-2P$
$R-2Q$	$726P = (\ 1\ ,\ 376)$	$=$	$(\ 1\ \ ,\ 376)$	$-P$
$R-2Q$	$726P = (\ 1\ ,\ 376)$	$\neq$	$(\ \infty\ \ ,\ \infty)$	0
$R-2Q$	$726P = (\ 1\ ,\ 376)$	$\neq$	$(\ 1\ \ ,\ 375)$	P
$R-2Q$	$726P = (\ 1\ ,\ 376)$	$\neq$	$(\ 2\ \ ,\ 378)$	$2P$
$R-2Q$	$726P = (\ 1\ ,\ 376)$	$\neq$	$(\ 6\ \ ,\ 361)$	$3P$
$R-2Q$	$726P = (\ 1\ ,\ 376)$	$\neq$	$(121\ ,\ 712)$	$4P$
$R-2Q$	$726P = (\ 1\ ,\ 376)$	$\neq$	$(\ 57\ ,\ 419)$	$5P$
$R-2Q$	$726P = (\ 1\ ,\ 376)$	$\neq$	$(\ 97\ ,\ 129)$	$6P$

$R-1Q$	$739P = (180\ ,\ 408)$	$\neq$	$(\ 57\ ,\ 332)$	$-5P$
$R-1Q$	$739P = (180\ ,\ 408)$	$\neq$	$(121\ ,\ 39)$	$-4P$
$R-1Q$	$739P = (180\ ,\ 408)$	$\neq$	$(\ 6\ \ ,\ 390)$	$-3P$
$R-1Q$	$739P = (180\ ,\ 408)$	$\neq$	$(\ 2\ \ ,\ 373)$	$-2P$
$R-1Q$	$739P = (180\ ,\ 408)$	$\neq$	$(\ 1\ \ ,\ 376)$	$-P$
$R-1Q$	$739P = (180\ ,\ 408)$	$\neq$	$(\ \infty\ \ ,\ \infty)$	0
$R-1Q$	$739P = (180\ ,\ 408)$	$\neq$	$(\ 1\ \ ,\ 375)$	P
$R-1Q$	$739P = (180\ ,\ 408)$	$\neq$	$(\ 2\ \ ,\ 378)$	$2P$
$R-1Q$	$739P = (180\ ,\ 408)$	$\neq$	$(\ 6\ \ ,\ 361)$	$3P$
$R-1Q$	$739P = (180\ ,\ 408)$	$\neq$	$(121\ ,\ 712)$	$4P$
$R-1Q$	$739P = (180\ ,\ 408)$	$\neq$	$(\ 57\ ,\ 419)$	$5P$
$R-1Q$	$739P = (180\ ,\ 408)$	$\neq$	$(\ 97\ ,\ 129)$	$6P$

$R-0Q$	$752P=(296\ ,\ 245)$	$\neq$	$(\ 97\ ,\ 215)$	$-6P$
$R-0Q$	$752P=(296\ ,\ 245)$	$\neq$	$(\ 57\ ,\ 332)$	$-5P$
$R-0Q$	$752P=(296\ ,\ 245)$	$\neq$	$(121\ ,\ 39)$	$-4P$
$R-0Q$	$752P=(296\ ,\ 245)$	$\neq$	$(\ 6\ \ ,\ 390)$	$-3P$
$R-0Q$	$752P=(296\ ,\ 245)$	$\neq$	$(\ 2\ \ ,\ 373)$	$-2P$
$R-0Q$	$752P=(296\ ,\ 245)$	$\neq$	$(\ 1\ \ ,\ 376)$	$-P$
$R-0Q$	$752P=(296\ ,\ 245)$	$\neq$	$(\ \infty\ \ ,\ \infty)$	0
$R-0Q$	$752P=(296\ ,\ 245)$	$\neq$	$(\ 1\ \ ,\ 375)$	P
$R-0Q$	$752P=(296\ ,\ 245)$	$\neq$	$(\ 2\ \ ,\ 378)$	$2P$
$R-0Q$	$752P=(296\ ,\ 245)$	$\neq$	$(\ 6\ \ ,\ 361)$	$3P$
$R-0Q$	$752P=(296\ ,\ 245)$	$\neq$	$(121\ ,\ 712)$	$4P$
$R-0Q$	$752P=(296\ ,\ 245)$	$\neq$	$(\ 57\ ,\ 419)$	$5P$
$R-0Q$	$752P=(296\ ,\ 245)$	$\neq$	$(\ 97\ ,\ 129)$	$6P$

$R+1Q$	$765P=(484\ ,\ 590)$	$\neq$	$(\ 57\ ,\ 332)$	$-5P$
$R+1Q$	$765P=(484\ ,\ 590)$	$\neq$	$(121\ ,\ 39)$	$-4P$
$R+1Q$	$765P=(484\ ,\ 590)$	$\neq$	$(\ 6\ \ ,\ 390)$	$-3P$
$R+1Q$	$765P=(484\ ,\ 590)$	$\neq$	$(\ 2\ \ ,\ 373)$	$-2P$
$R+1Q$	$765P=(484\ ,\ 590)$	$\neq$	$(\ 1\ \ ,\ 376)$	$-P$
$R+1Q$	$765P=(484\ ,\ 590)$	$\neq$	$(\ \infty\ \ ,\ \infty)$	0
$R+1Q$	$765P=(484\ ,\ 590)$	$\neq$	$(\ 1\ \ ,\ 375)$	P
$R+1Q$	$765P=(484\ ,\ 590)$	$\neq$	$(\ 2\ \ ,\ 378)$	$2P$
$R+1Q$	$765P=(484\ ,\ 590)$	$\neq$	$(\ 6\ \ ,\ 361)$	$3P$
$R+1Q$	$765P=(484\ ,\ 590)$	$\neq$	$(121\ ,\ 712)$	$4P$
$R+1Q$	$765P=(484\ ,\ 590)$	$\neq$	$(\ 57\ ,\ 419)$	$5P$
$R+1Q$	$765P=(484\ ,\ 590)$	$\neq$	$(\ 97\ ,\ 129)$	$6P$

$R+2Q$	$778P = (508\ ,\ 668)$	$\neq$	$(\ 97\ ,\ 215)$	$-6P$
$R+2Q$	$778P = (508\ ,\ 668)$	$\neq$	$(\ 57\ ,\ 332)$	$-5P$
$R+2Q$	$778P = (508\ ,\ 668)$	$\neq$	$(121\ ,\ 39)$	$-4P$
$R+2Q$	$778P = (508\ ,\ 668)$	$\neq$	$(\ 6\ \ ,\ 390)$	$-3P$
$R+2Q$	$778P = (508\ ,\ 668)$	$\neq$	$(\ 2\ \ ,\ 373)$	$-2P$
$R+2Q$	$778P = (508\ ,\ 668)$	$\neq$	$(\ 1\ \ ,\ 376)$	$-P$
$R+2Q$	$778P = (508\ ,\ 668)$	$\neq$	$(\ \infty\ \ ,\ \infty)$	0
$R+2Q$	$778P = (508\ ,\ 668)$	$\neq$	$(\ 1\ \ ,\ 375)$	P
$R+2Q$	$778P = (508\ ,\ 668)$	$\neq$	$(\ 2\ \ ,\ 378)$	$2P$
$R+2Q$	$778P = (508\ ,\ 668)$	$\neq$	$(\ 6\ \ ,\ 361)$	$3P$
$R+2Q$	$778P = (508\ ,\ 668)$	$\neq$	$(121\ ,\ 712)$	$4P$
$R+2Q$	$778P = (508\ ,\ 668)$	$\neq$	$(\ 57\ ,\ 419)$	$5P$
$R+2Q$	$778P = (508\ ,\ 668)$	$\neq$	$(\ 97\ ,\ 129)$	$6P$

$R+3Q$	$791P = (720\ ,\ 570)$	$\neq$	$(\ 57\ ,\ 332)$	$-5P$
$R+3Q$	$791P = (720\ ,\ 570)$	$\neq$	$(121\ ,\ 39)$	$-4P$
$R+3Q$	$791P = (720\ ,\ 570)$	$\neq$	$(\ 6\ \ ,\ 390)$	$-3P$
$R+3Q$	$791P = (720\ ,\ 570)$	$\neq$	$(\ 2\ \ ,\ 373)$	$-2P$
$R+3Q$	$791P = (720\ ,\ 570)$	$\neq$	$(\ 1\ \ ,\ 376)$	$-P$
$R+3Q$	$791P = (720\ ,\ 570)$	$\neq$	$(\ \infty\ \ ,\ \infty)$	0
$R+3Q$	$791P = (720\ ,\ 570)$	$\neq$	$(\ 1\ \ ,\ 375)$	P
$R+3Q$	$791P = (720\ ,\ 570)$	$\neq$	$(\ 2\ \ ,\ 378)$	$2P$
$R+3Q$	$791P = (720\ ,\ 570)$	$\neq$	$(\ 6\ \ ,\ 361)$	$3P$
$R+3Q$	$791P = (720\ ,\ 570)$	$\neq$	$(121\ ,\ 712)$	$4P$
$R+3Q$	$791P = (720\ ,\ 570)$	$\neq$	$(\ 57\ ,\ 419)$	$5P$
$R+3Q$	$791P = (720\ ,\ 570)$	$\neq$	$(\ 97\ ,\ 129)$	$6P$

$R+4Q$	$804P = (47\ ,\ 335)$	$\neq$	$(97\ ,\ 215)$	$-6P$
$R+4Q$	$804P = (47\ ,\ 335)$	$\neq$	$(57\ ,\ 332)$	$-5P$
$R+4Q$	$804P = (47\ ,\ 335)$	$\neq$	$(121\ ,\ 39)$	$-4P$
$R+4Q$	$804P = (47\ ,\ 335)$	$\neq$	$(6\ ,\ 390)$	$-3P$
$R+4Q$	$804P = (47\ ,\ 335)$	$\neq$	$(2\ ,\ 373)$	$-2P$
$R+4Q$	$804P = (47\ ,\ 335)$	$\neq$	$(1\ ,\ 376)$	$-P$
$R+4Q$	$804P = (47\ ,\ 335)$	$\neq$	$(\infty\ ,\ \infty)$	0
$R+4Q$	$804P = (47\ ,\ 335)$	$\neq$	$(1\ ,\ 375)$	P
$R+4Q$	$804P = (47\ ,\ 335)$	$\neq$	$(2\ ,\ 378)$	$2P$
$R+4Q$	$804P = (47\ ,\ 335)$	$\neq$	$(6\ ,\ 361)$	$3P$
$R+4Q$	$804P = (47\ ,\ 335)$	$\neq$	$(121\ ,\ 712)$	$4P$
$R+4Q$	$804P = (47\ ,\ 335)$	$\neq$	$(57\ ,\ 419)$	$5P$
$R+4Q$	$804P = (47\ ,\ 335)$	$\neq$	$(97\ ,\ 129)$	$6P$

Apéndice A

PRELIMINARES DE TEORÍA DE NÚMEROS

En este trabajo supondremos que el lector tiene conocimientos básicos sobre divisibilidad. En particular supondremos que conoce el algoritmo de la división, las propiedades sencillas de las congruencias y el Teorema Chino del Residuo. Como más adelante necesitaremos la función ϕ de Euler y sus principales cualidades, en esta sección las desarrollaremos.

DEFINICIÓN 1 Dado un número natural n se define la *función ϕ de Euler* por medio de la siguiente igualdad:

$$\phi(n) = \#(\{m \in \mathbb{N} : (n, m) = 1 \text{ y } 1 \leq m \leq n\}).$$

En el caso en que $n > 1$, n no es primo relativo con n, de manera que podemos poner

$$\phi(n) = \#(\{m \in \mathbb{N} : (n, m) = 1 \text{ y } 1 \leq m < n\})$$

PROPOSICIÓN 2

(a) Si p es un número primo, entonces $\phi(p) = p - 1$.

(b) La función ϕ es multiplicativa. Esto es, si $(m, n) = 1$, entonces $\phi(nm) = \phi(n)\phi(m)$.

(c) Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ es la factorización de n como producto de primos, entonces

$$\phi(n) = n(1 - \tfrac{1}{p_1})(1 - \tfrac{1}{p_2}) \cdots (1 - \tfrac{1}{p_k}).$$

DEMOSTRACIÓN.

(a) Si p es primo, entonces todos los números $1, 2, ..., p-1$ son primos relativos con p, mientras que p no es primo relativo con él mismo. De manera que $\{m \in \mathbb{N} : (n, m) = 1 \text{ y } 1 \leq m \leq n\} = \{1, 2, ..., p - 1\}$, por lo que $\phi(p) = p - 1$.

(b) Tomemos $n, m \in \mathbb{N}$ tales que $(n, m) = 1$. Podemos suponer que ninguno de los números n y m es igual a 1. Sean $r = \phi(n)$ y $s = \phi(m)$. Denotemos por $a_1, a_2, ..., a_r$ a los diferentes números del conjunto $\{k \in \mathbb{N} : (n, k) = 1 \text{ y } 1 \leq k < n\}$ y por $b_1, b_2, ..., b_s$ a los del conjunto $\{k \in \mathbb{N} : (m, k) = 1 \text{ y } 1 \leq k < m\}$.

Dado un elemento $k \in \mathbb{N}$ tal que $(mn, k) = 1$ y $1 \leq k \leq mn$, tenemos que k no tiene ningún divisor, mayor que 1, común con mn, menos lo va a tener con n y con m. Es decir, $(m, k) = 1$ y $(n, k) = 1$. Sea u el residuo de dividir a k entre n. Entonces $k = nq + u$, donde q es un entero y $0 \leq u < n$. No es posible que n y u tengan un divisor común mayor que 1 pues éste también tendría que dividir a k. De modo que $(n, u) = 1$. Por tanto u tiene que ser uno de los elementos de la forma a_i. En forma similar se muestra que el residuo de dividir a k entre m es igual a uno de los números b_j. Notemos que $k \equiv a_i (\text{mod } n)$ y $k \equiv b_j (\text{mod } m)$. Como el residuo siempre es único, podemos establecer una función del conjunto $A = \{k \in \mathbb{N} : (mn, k) = 1 \text{ y } 1 \leq k < mn\}$ en el conjunto de parejas $\{(a_i, b_j) : i \in \{1, ..., r\} \text{ y } j \in \{1, ..., s\}\}$.

El Teorema Chino del Residuo implica que el sistema de congruencias

$$h \equiv a_i \pmod{n} \quad \text{y} \quad h \equiv b_j \pmod{m}$$

tiene una única solución módulo mn. En particular, hay una única $h \in \{0, 1, ..., mn-1\}$ que satisface tal sistema.

Esto nos dice que para dos números diferentes k en A, la pareja de sus residuos (a_i, b_j) es única, pues de lo contrario tendríamos dos soluciones para el sistema mencionado. Por tanto la función que estamos proponiendo es inyectiva.

Nos falta mostrar que la función es suprayectiva. Tomemos una pareja (a_i, b_j). Por el Teorema Chino del Residuo, existe una $h \in \{0, 1, ..., mn-1\}$ tal que se satisface el sistema de arriba. La congruencia $h \equiv a_i \pmod{n}$ implica que $h = nq + a_i$ para algún entero q, de modo que a_i es el residuo de h módulo n. Similarmente, b_j es el residuo de h módulo m. Sólo nos falta ver que h pertenece a A, para lo cual nos falta verificar que $(h, nm) = 1$. La igualdad $h = nq + a_i$ y el hecho de que $(n, a_i) = 1$ implican que $(n, h) = 1$. Similarmente, $(m, h) = 1$. Esto implica que $(mn, h) = 1$. Por tanto $h \in A$.

Hemos establecido entonces una biyección entre A y el conjunto de parejas. El número de elementos de A es, por definición, igual a $\phi(mn)$ y el número de parejas es igual a $\phi(m)\phi(n)$. Por tanto, podemos concluir que $\phi(mn) = \phi(m)\phi(n)$.

(c) Supongamos que $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ es la factorización de n como producto de primos. Esto quiere decir, en particular, que todos los p_i son diferentes. Entonces los números $p_i^{\alpha_i}$ son primos relativos entre sí. De manera que $\phi(n) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2}) \cdots \phi(p_k^{\alpha_k})$. Por tanto, sólo nos tenemos que preocupar por saber calcular ϕ en un número de la forma p^α, donde p es un primo y $\alpha \in \mathbb{N}$.

Notemos que los únicos números que no son primos relativos con p^α son precisamente los múltiplos de p. De modo que

$$\begin{aligned} & \{m \in \mathbb{N} : (p^\alpha, m) = 1 \text{ y } 1 \leq m \leq p^\alpha\} \\ = \; & \{1, 2, ..., p^\alpha\} - \{p, 2p, ..., p^\alpha = p^{\alpha-1}p\}. \end{aligned}$$

Así que $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Ya estamos en condiciones de calcular $\phi(n)$. Haciéndolo nos queda:

$$\begin{aligned}\phi(n) &= \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2})\cdots\phi(p_k^{\alpha_k}) \\ &= (p_1^{\alpha_1} - p_1^{\alpha_1-1})(p_2^{\alpha_2} - p_2^{\alpha_2-1})\cdots(p_k^{\alpha_k} - p_k^{\alpha_k-1}) \\ &= p_1^{\alpha_1}(1 - \frac{1}{p_1})p_2^{\alpha_2}(1 - \frac{1}{p_2})\cdots p_k^{\alpha_k}(1 - \frac{1}{p_k}) \\ &= n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})\cdots(1 - \frac{1}{p_k}).\end{aligned}$$

Y esto termina la demostración de la proposición.

■

TEOREMA 3 . Si b y m son números naturales tales que $(b, m) = 1$, entonces $b^{\phi(m)} \equiv 1 (\text{mod } m)$.

DEMOSTRACIÓN.

Sean $a_1, a_2, ..., a_r$ los diferentes elementos del conjunto $A = \{k \in \mathbb{N} : (m, k) = 1 \text{ y } 1 \leq k < m\}$. Por definición $r = \phi(m)$. Para cada elemento de la forma ba_i, tomemos su residuo u_i, de dividirlo entre m. Entonces $ba_i = mq_i + u_i$ para algún entero q_i. Además $ba_i \equiv u_i (\text{mod } m)$. Como b y a_i son primos relativos con m, también lo es su producto. Esto implica que u_i también es primo relativo con m. De manera que u_i también pertenece a A por lo que es igual a un a_{j_i}. Como el residuo de dividir natural entre otro es único, tenemos definida una función que a cada ba_i le asocia a_{j_i}.

Si a ba_i y a ba_k les correspondiera la misma a_j, tendríamos que $ba_i \equiv a_{j_i} = a_{j_k} \equiv ba_k$, todo módulo m. Así que $ba_i \equiv ba_k (\text{mod } m)$. Ya que $(b, m) = 1$, el número b tiene inverso multiplicativo módulo m, por lo que en la última congruencia, b puede ser eliminado, con lo que tendríamos que $a_i \equiv a_k (\text{mod } m)$. Ya que ambos elementos a_i y a_k están entre 0 y $m - 1$, esta última congruencia sólo es posible si $a_i = a_k$ y, entonces $i = k$. Esto prueba que la asociación es inyectiva.

Por tanto tenemos una función inyectiva del conjunto $\{ba_1, ba_2, ..., ba_r\}$ en el conjunto $\{a_1, a_2, ..., a_r\}$. Como ambos conjuntos tienen el mismo número

de elementos, tal función tiene que ser suprayectiva. Entonces los elementos $a_{j_1}, a_{j_2}, ..., a_{j_r}$ tienen que ser los mismos que $a_1, a_2, ..., a_r$, salvo que quizá estén en diferente orden. Así que si los multiplicamos todos obtendremos el mismo resultado. Por tanto:

$$b^r a_1 a_2 \cdots a_r = ba_1 ba_2 \cdots ba_r \equiv a_{j_1} a_{j_2} \cdots a_{j_r} = a_1 a_2 \cdots a_r (\text{mod } m).$$

Entonces

$$b^r a_1 a_2 \cdots a_r \equiv a_1 a_2 \cdots a_r (\text{mod } m).$$

Como los a_i son primos relativos con m, se pueden ir cancelando de esta congruencia hasta obtener:

$$b^r \equiv 1 (\text{mod } m).$$

Que es exactamente lo que pretendíamos demostrar. ■

COROLARIO 4 Si a, p son números naturales tales que p es primo y p no divide a a, entonces $a^{p-1} \equiv 1 (\text{mod } p)$.

Bibliografía

[1] Ahlgors Lars V. *Complex analisys, An introduction to the theory of analytic functions of one complex variable. Third edition.* McGraw Hill book company.1979.

[2] Haseer, N. B., LaSalle, J. P. y Sullivan, J. A. *Análisis Matemático, Curso Intermedio, vol. 2.* Trillas, México, 1990.

[3] Herstein, I. N. *Álgebra Moderna* Trillas, México, 1980.

[4] Pino Caballero Gil. *Introducción a la Criptografía 2a. edición actualizada.* Algaomega Grupo Editor, 2003.

[5] Silverman, J. H. *The Arithmetic of Elliptic Curves. (Graduate texts in mathmatics; 106).* Springer, USA, 1985.

[6] Wunsch, A. David. *Variable compleja con aplicaciones, 2a. edición.* Addison-Wesley Iberoamericana, U.S.A., 1997.