UNIVERSIDAD DEL BÍO-BÍO

FACULTAD DE EDUCACIÓN Y HUMANIDADES

DEPARTAMENTO DE CIENCIAS DE LA EDUCACÓN

ESCUELA DE PEDAGOGÍA EN EDUCACIÓN MATEMÁTICA

CURVAS ELÍPTICAS Y TEST DE PRIMALIDAD

MEMORIA PARA OPTAR AL TÍTULO DE PROFESOR/A DE EDUCACIÓN MEDIA EN EDUCACIÓN MATEMÁTICA

AUTORES: GAJARDO RAMÍREZ, STEFANY ARACELY
VÁSQUEZ CEA, YOSELYN FRANCISCA
ZENTENO ACUÑA, CRISTIAN

Profesor Guía: Riquelme Faúndez, Edgardo Andrés

CHILLÁN 2019

Resumen

La siguiente memoria se focaliza en el estudio de test de primalidad, especialmente el Goldwasser-Killian que utiliza curvas elípticas, y su posterior implementación utilizando Magma.

Antes de comenzar directamente con el estudio de el test de primalidad previamente mencionado, es necesario hacer una revisión de los fundamentos matemáticos en el área de álgebra abtracta, particularmente teoría de grupos, anillos, cuerpos finitos. espacio proyectivo y punto en el infinito. Del mismo modo, se realizará un recorrido por distintos y destacados test de primalidad, dentro de los que se encuentran, por ejemplo, el test probabilístico de primalidad Miller-Rabin.

Posteriormente, para desarrollar correctamente el test y sus aplicaciones, se debe estudiar el concepto de curvas elípticas sobre cuerpos finitos y la j-invariante, no sin antes revisar los axiomas de grupo que cumple la suma de puntos de una curva elíptica.

Finalmente estudiaremos el test Goldwasser-killian que está entre los métodos más rápidos y más ampliamente utilizados en probar primalidad y aplicaremos los algoritmos en Magma, que es un sistema algebraico computacional diseñado especialmente para resolver problemas de álgebra abstracta, teoría de números, geometría algebraica y combinatoria.

Simbología

Símbolo	Significado
$(R, +)$	Conjunto asociado a la adición
R^*	Elementos invertibles de R
e	Elemento neutro multiplicativo
$-a$	Inverso aditivo de a
a^{-1}	Inverso multiplicativo de a
0	Elemento neutro aditivo
$\|G\|$	Orden del grupo G
$A \simeq B$	A es isomorfo a B
$mcm(a, b)$	Mínimo común múltiplo entre a y b
$mcd(a, b)$	Máximo común divisor
$\mathbb{F}_q$	Cuerpo de q elementos
$P(x)$	Polinomio P de incógnita x
$\mathbb{Z}/n\mathbb{Z}$	$\mathbb{Z}$ cocientado por $n\mathbb{Z}$
$\overline{\mathbb{K}}$	Clausura algebraica de $\mathbb{K}$
$\frac{\delta f}{\delta x}$	Derivada de f respecto de x
$\triangle$	Discriminante
$\oplus$	Suma elíptica
$\#E$	Cardinalidad de E
$(x : y : 0)$	Punto en el infinito de una curva elíptica

Índice general

Introducción

Historia y aplicaciones: Conexión con enseñanza media

La búsqueda de números primos grandes no es una tarea fácil porque todavía nadie ha sido capaz de encontrar la fórmula que nos permita construir números primos. Frente a esto, algunas personas se pueden preguntar: ¿Para qué queremos construir números primos? Existen dos respuestas a esta interrogante.

La primera respuesta se relaciona con un interés teórico. El intento promueve el nacimiento de herramientas de cálculo interesantes, especialmente de cálculo informático. Además, conocer un listado extenso de números primos nos permite comprobar teoremas que aún no han sido demostrados. Si algún matemático crea una conjetura sobre números primos y se puede comprobar que hay uno, independiente de la cantidad de cifras que tenga el número, que no la cumple, la conjetura queda concluida. Esto ha desencadenado una búsqueda de números primos de todas familias, de Mersenne, gemelos, etc., que en algunos casos ha llegado a tener un carácter que podríamos calificar de competitivo, inscrito en el mundo de los récords y de los grandes premios.

La segunda respuesta a la interrogante es de índole práctica, que guarda estrecha relación con algo muy utilizado en el área informática y que se encuentra presente en la sociedad actual sin que lo notemos, las llamadas claves criptográficas: el correo electrónico, las transacciones bancarias, las tarjetas de crédito o las comunicaciones por teléfono celular se protegen mediante claves secretas que se basan directamente en las propiedades de los números primos.

Los números primos son tratados en el sistema escolar de forma implícita desde 5º año básico, ya que en este nivel los estudiantes comienzan a realizar operaciones con fracciones y para la suma de ellas, los niños deben calcular mínimo común múltiplo entre los denominadores, y al realizar este procedimiento los alumnos descomponen un número compuesto en factores primos.

En 6º año básico según el currículo nacional los estudiantes deben identificar números primos y compuestos. En el texto escolar se definen los números primos y descomposición prima, siendo éste el único curso en donde se trabajan los números primos de forma explícita. Desde 7º año básico en adelante los estudiantes siguen trabajando con fracciones hasta que acaba la enseñanza escolar.

Los números primos de gran tamaño, pueden emplearse para codificar cualquier tipo de información de manera segura. Si se escogen un par de números grandísimos primos y se multiplican, el camino inverso, de descomposición del número compuesto en factores primos, es un tanto complejo. Esto lo usan los bancos en los números de seguridad, las transferencias bancarias y otras operaciones.

Por otra parte, la enseñanza y utilidad de los números primos, se relaciona con la utilización de software matemáticos, que pueden ser usados para promover el trabajo colaborativo y estimular el reconocimiento del uso de los números primos en la vida cotidiana y su importancia en el desarrollo de los sistemas computacionales desde sus inicios hasta el día de hoy.

Estimular la búsqueda y selección crítica de información proveniente de diferentes soportes, la evaluación y validación, el procesamiento, la jerarquización, la crítica y la interpretación, son algunos de los objetivos de la enseñanza de los números primos y la búsqueda de aquellos de gran tamaño según la planificación de actividades que se elaboren entorno a ellos.

CAPÍTULO 1

Fundamentos Matemáticos

En este capítulo se definirán conceptos preliminares de teoría de números y álgebra abstracta para adquirir conocimientos previos y comprender las curvas elípticas junto a los test de primalidad que estudiaremos en este trabajo. Específicamente se tratará la teoría de Grupos, Anillos y Cuerpos de orden finito para dar una base teórica al estudio. Otro concepto importante que estudiaremos en este capítulo es el de espacios proyectivos, que nos permite interpretar lo que es un punto en el infinito de una curva elíptica.

1.1 Grupos Abelianos Finitos

En esta sección, comenzaremos con dos proposiciones básicas de los cursos de teoría de números:

Proposición 1.1. *En los grupos cíclicos, todo grupo de orden primo es isomorfo a $\mathbb{Z}_p$, donde p es un número primo.*

Proposición 1.2. $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ *cuando* $mcd(m,n) = 1$.

Definición 1.1. *Supongamos que G es un grupo y sea g_i un conjunto de elementos en G, con i en algún conjunto de índices I (no necesariamente finito). El menor subgrupo de G que contenga todos los g_i es un subgrupo de G generado por los g_i. Si este subgrupo de G es todo G, entonces G es generado por el conjunto $\{g_i : i \in I\}$. Entonces g_i son generadores de G. Si existe un conjunto finito $\{g_i : i \in I\}$ que genere a G, entonces G es finitamente generado.*

Proposición 1.3. *Sea H el subgrupo de un grupo G generado por $\{g_i \in G : i \in I\}$. Entonces $h \in H$ si y solo si es un producto de la forma*

$$h = {g_{i_1}}^{a_1} ... {g_{i_n}}^{a_n}$$

donde los g_{i_k} no son necesariamente diferentes.

Demostración 1.1. Sea K el conjunto de todos los productos de la forma $g_{i_1}^{\alpha_1} \cdots g_{i_n}^{\alpha_n}$, donde los g_{i_k} no son necesariamente diferentes. Y sea K es un subconjunto de H. Si K es un subgrupo de G, entonces $K = H$, pues H es el menor subgrupo que contiene todos los g_i.
K es cerrado bajo la operación del grupo. Como $g_i^0 = 1$, la identidad está en K. Falta mostrar que el inverso de un elemento $g = g_{i_1}^{k_1} \cdots g_{i_n}^{k_n}$ en K también está en K. Pero,

$$g = (g_{i_1}^{k_1} \cdots g_{i_n}^{k_n})^{-1} = (g_{i_n}^{-k_n} \cdots g_{i_1}^{-k_1})$$

Se puede expresar cualquier grupo abeliano finito como un producto directo finito de grupos cíclicos. Si p es un número primo, diremos que un grupo G es un p-grupo si todo elemento en G tiene como su orden una potencia de p.

Ejemplo 1.1.1. *$\mathbb{Z}_2 \times \mathbb{Z}_2$ como $\mathbb{Z}_4$ es 2-grupo, mientras $\mathbb{Z}_{27}$ es un 3-grupo.*

Teorema 1.1. ***Teorema fundamental de los grupos abelianos finitos.*** *Todo grupo abeliano finito G es isomorfo a un producto directo de grupos ciclicos de la forma*

$$\mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_n^{a_n}}$$

los p_i son primos (no necesariamente diferentes).

La demostración del Teorema Fundamental de los Grupos Abelianos Finitos depende de varios lemas.

Lema 1.1. *Sea G un grupo abeliano finito de orden n. Si p es un primo que divide a n, entonces G contiene un elemento de orden p.*

Demostración 1.2. Demostraremos este lema por inducción. Si $n = 1$, entonces no hay nada que demostrar. Ahora supongamos que el orden de G es n y que el lema es verdadero para todos los grupos de orden k donde $k < n$. Más aún, sea p un número primo que divide a n.

Si G no tiene subgrupos triviales, entonces $G =< a >$, donde a es cualquier elemento distinto de la identidad.

Ahora supongmos que G contiene un subgrupo no trivial propio H. Entonces $1 < |H| < n$. Si $p||H|$, entonces H contiene un elemento de orden p por la hipotesis de inducción y el lema se cumple para G.
Supongamos que p no divide al orden de H. Como G es abeliano, H es un

subgrupo normal de G, y $|G| = |H| \cdot |G/H|$. De manera que p divide a $|G/H|$. Como $|G/H| < |G| = n$, sabemos que G/H que contiene un elemento aH de orden p por la hipótesis de inducción. Luego,

$$H = (aH)^p = a^p H$$

, y $a^p \in H$ pero $a \notin H$. Si $|H| = r$, entonces p y r son relativamente primos, y existen enteros primos s y t tales que $sp+tr = 1$. Además, el orden de a^p divide a r, y $(a^p)^r = (a^r)^p = 1$.

Afirmamos que a^r tiene orden p. Debemos mostrar que $a^r \neq 1$.
Supongamos que $a^r = 1$. Entonces,

$$a = a^{sp+tr}$$

$$= a^{sp}a^{tr}$$

$$= (a^p)^s(a^r)^t$$

$$= (a^p)^s e$$

$$= (a^p)^s$$

Como $a^p \in H$, tenemos que $a = (a^p)^s \in \mathbb{H}$, lo que es una contradicción. Por lo tanto, $a^r \neq 1$ es un elemento de orden $p \in G$.

Lema 1.2. *Un grupo abeliano finito es un $p-$ grupo si y sólo si su orden es una potencia de p.*

Demostración 1.3. Si $|G| = p^n$ entonces, por el teorema de Lagrange, el orden de cualquier $g \in G$ divide a p^n, y por lo tanto es una potencia de p. Recíprocamente, si $|G|$ no es una potencia de p, entonces tiene algún otro divisor primo q, y por el lema 3.1, G tiene un elemento de orden q por lo que no es un $p-$ *grupo.*

Lema 1.3. *Sea G un grupo abeliano finito de orden $n = {p_1}^{a_1}...p_k^{a_k}$, con $p_1, 2..., p_k$ primos distintos y $a_1, a_2, ..., a_k$ enteros positivos. Entonces G es el producto directo interno de subgrupos $G_1, G_2, ..., G_k$, donde G_i es el subgrupo de G que consiste de todos los elementos de orden p_i^k para algún entero k.*

Demostración 1.4. Como G es un grupo abeliano, tenemos que G_i es un grupo G para $i = 1, ..., n$. Como la identidad tiene orden $p_i^0 = 1$, sabemos que $1 \in G_i$. Si $g \in G$ tiene orden p_i^r, entonces g^{-1} también debe tener orden p_i^r.

Finalmente, si $h \in G_i$ tiene orden p_i^s, entonces

$$(gh)^{p_i^t} = p^{p_i^t}h^{p_i^t} = 1 \cdot 1 = 1$$

donde t es el mayor entre r y s.
Debemos demostrar que

$$G = G_1 G_2 \cdots G_n$$

y $G_i \cap G_j = \{1\}$ para $i \neq j$. Supongamos que $g_1 \in G_1$ esta en el subgrupo generado por $G_2, G_3, ..., G_k$. Entonces $g_1 = g_2 g_3 \cdots g_k$ para $g_i \in G_i$. Como g_i tiene orden p^{α_i} sabemos que $g_i^{p^{\alpha_i}} = 1$ para $i = 2, 3, ..., k$ y $g_1^{p_2^{\alpha_2} \cdots p_k^{\alpha_k}} = 1$. Como el orden de g_1 es una potencia de p_1 y $mcd(p_1, p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = 1$, tenemos $g_1 = 1$ y la intersección de G_1 con cualquuiera de los subgrupos $G_2, G_3 \cdots G_k$ es la identidad. Un argumento similar muestra que $G_i \cap Gj = \{1\}$ para $i \neq j$. Luego $G_1 G_2 \cdots G_n$ es un producto directo interno de subgrupos. Como

$$|G_2 G_3 \cdots G_k| = p_1^{\alpha_1} \cdot p_k^{\alpha_k} = |G|$$

Tenemos que $G = G_1 G_2 \cdots G_k$.

Lema 1.4. *Sea G un $p-$ grupo abeliano finito y supongamos que $g \in G$ tiene orden maximal. Entonces G es isomorfo a $\langle g \rangle \times H$ para algún H de G.*

Teorema 1.2. ***Teorema Fundamental de los Grupos Abelianos Finitamente Generados (divisores elementales)*** *Todo grupo abeliano finitamente generado G es isomorfo a un producto directo de grupos cíclicos de la forma*

$$\mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times ... \times \mathbb{Z}_{p_n^{a_n}} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

, donde los p_i son primo (no necesariamente distintos).

1.2 Anillos

Definición 1.2. *Un anillo A es un conjunto dotado de dos operaciones binarias $+$ y $\cdot$, que llamaremos suma y producto, definidas en A tales que se satisfacen los siguientes axiomas:*

1. *$(A, +)$ es un grupo abeliano.*
2. *La multiplicación es asociativa.*
3. *Para todas las $a, b, c \in A$ se cumple la:*
   - ***ley distributiva izquierda*** $a(b + c) = (ab) + (ac)$
   - ***ley distributiva derecha*** $(a + b)c = (ac) + (bc)$

Sabiendo que existen distintos axiomas de grupo, válidos para cada operación, es importante definir aquellas variaciones que obtiene el anillo al cumplir adicionalmente alguno o algunos de los axiomas restantes para la operación producto.

Ejemplo 1.2.1. *Sea $A = \mathbb{Z}$ con la suma y el producto usuales forman un anillo. Además, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ con la suma y el producto usuales son un anillo.*

Definición 1.3. ***Anillo conmutativo*** *Se dice que un anillo A es conmutativo si y solo si*

$$\forall\ a, b \in A^* \qquad a \cdot b = b \cdot a$$

Se cumple la propiedad conmutativa para el producto.

Ejemplo 1.2.2. *$A = M_{nxm}(\mathbb{R})$ con la suma y el producto usuales de matrices forman un anillo que no es conmutativo.*

Definición 1.4. ***Anillo con uno****. Un anillo A es un anillo con uno si y solo si posee el elemento neutro para el producto.*

Ejemplo 1.2.3. *El conjunto de $F[x]$ de los polinomios con los coeficientes en $\mathbb{Z}$, con la adición y multiplicacion usual son un anillo con uno.*

Definición 1.5. ***Anillo de división****. Un anillo de división es un anillo con uno en el que todo elemento del anillo distinto de cero (es decir, distinto del elemento neutro aditivo) es invertible.*

$$\forall\ a \in A^*\ \exists!\ b \in A^*,\ \textit{tal que}\ \ a \cdot b = e$$

En $\mathbb{Z}$ es cierto que si $a \cdot b = 0$ entonces $a = 0$ o $b = 0$, sin embargo ello deja de ser válido en general.

Ejemplo 1.2.4. *$\mathbb{Z}_8$ anillo conmutativo con uno.*
$\mathbb{Z}_8^* = \{1, 3, 5, 7\}$ (primos relativos con 8), por lo tanto $\mathbb{Z}_8$ no es un anillo de división.

Definición 1.6. ***Divisores de 0****. Dado un anillo A y $a \in A$ con $a \neq 0$ se dice que es un divisor de cero si existe un elemento $b \in A$ y $b \neq 0$ tal que $a \cdot b = 0$ o $b \cdot a = 0$.*

Ejemplo 1.2.5. *En $\mathbb{Z}_{10}$ se tiene que $\bar{2} \neq \bar{0}$ y $\bar{5} \neq \bar{0}$, pero $\bar{2} \cdot \bar{5} = \bar{10} = \bar{0}$ en $\mathbb{Z}_{10}$*

Definición 1.7. ***Dominio entero****. Un anillo conmutativo con uno A es un dominio entero cuando no existen divisores de cero en el anillo. Es decir, dados $a, b \in A$ tal que $a \cdot b = 0$ implica que $a = 0$ o $b = 0$.*

Ejemplo 1.2.6. $(\mathbb{Z}, +, \cdot)$

Definición 1.8. ***Característica de un anillo****. Sea A un anillo cualquiera, Si existe un entero positivo n, tal que $na = 0$ para todo $a \in A$ donde n es el entero positivo más pequeño con esta propiedad, este es llamado característica del anillo. Si no existe ese entero positivo (esto es, si $na = 0$ para todas las $a \in A$ implica $n = 0$) entonces decimos que el anillo tiene característica 0.*

Teorema 1.3. *Si A es un anillo con uno, entonces A tiene característica $n > 0$ si y solo si n es el menor entero positivo tal que $n \cdot 1 = 0$.*

Demostración 1.5. Por definición, si A tiene característica $n > 0$ entonces $na = 0$ para todas las $a \in A$ en particular $n \cdot 1 = 0$

Supongase que n es el menor entero tal que $n \cdot 1 = 0$ entonces para cualquier $a \in A$ tenemos que

$$n \cdot a = a + a + ... + a = a(1 + 1 + ... + 1) = a(n \cdot 1) = a \cdot 0 = 0$$

Corolario 1.1. *La característica de un dominio entero A es cero o un número primo*

Demostración 1.6. Sea A un anillo con característica n y asumiendo un n compuesto, por lo que n se puede escribir como $n = n_1 \cdot n_2$ con $1 < n_i < n$, $(i = 1, 2)$.
Obteniendo

$$0 = n \cdot 1 = (n_1 \cdot n_2)1 = (n_1 \cdot n_2)1^2 = (n_1 1) \cdot (n_2 1)$$

Por hipótesis se tiene que A no tiene divisores de 0, por lo que $n_1 1 = 0$ o $n_2 1 = 0$, pero esto contradice la elección de n, ya que el entero positivo más pequeño tal que $n1 = 0$. Por lo tanto, la característica debe ser un número primo.

Entonces si la característica no es un número primo y no puede ser un número compuesto (por lo anterior) sólo queda la posibilidad que sea 0.

1.2.1 Ideales y anillos cocientes

Dentro del anillo, al igual que en un grupo podemos encontrar subconjuntos del anillo que cumplen las mismas propiedades, así como en un grupo podemos

encontrar subgrupos, en anillos podemos encontrar subanillos.
En el caso de los subanillos podemos encontrar ciertos casos que son importantes para futuras definiciones, como lo son:

Definición 1.9. ***Ideal***

Se dice que un Ideal I es un subgrupo aditivo $(I,+)$ de un anillo A que satisface $aI \subseteq I$ y $Ia \subseteq I$ para todas las $a \in A$. (Un ideal es a un anillo como un subgrupo normal es a un grupo).

Ejemplo 1.2.7. *Para todo entero relativo $k, k\mathbb{Z}$ es un ideal de $\mathbb{Z}$*

Definición 1.10. ***Ideal maximal*** *Se dice que un ideal I no trivial de un anillo A es maximal si y solo si no está contenido en ningún otro ideal.*

Ejemplo 1.2.8. *En el anillo $\mathbb{Z}$, es sencillo de verificar que $J = p\mathbb{Z}(pprimo)$, es un ideal maximal de $\mathbb{Z}$*

Definición 1.11. ***Ideal primo*** *Un ideal I distinto de un anillo conmutativo A, es un ideal primo si $ab \in I$ implica que $a \in I$ o $b \in I$ para todas las $a, b \in A$.*

Definición 1.12. ***Anillo cociente*** *Si I es un ideal en un anillo A entonces el anillo de las clases laterales $a + I$ bajo las operaciones de clases, es el anillo cociente. Este anillo se denota por A/I*

En particular, el cociente A/I es un grupo respecto a la suma de clases:

$$(r + I) + (s + I) = (r + s) + I$$

y en analogía con esto se tiene una definición de un producto de clases:

$$(r + I)(s + I) = rs + I$$

Pero es natural cuestionarse sobre si las operaciones están bien definidas, es decir, si es independiente de la elección de un representante en cada una de las clases.
Para la suma, es evidente que está bien definida, pues $(I,+)$ es subgrupo normal de $(A,+)$. Para la multiplicación, tomamos dos clases; $(r+I)$ y $(s+I)$, entonces la multiplicación de clases se puede realizar utilizando la propiedad distributiva del anillo

$$(r + I)(s + I) = rs + rI + sI + I$$

pero como I es un ideal, los elementos rI, sI, $I \in A$, entonces el producto de dos clases queda definido como:

$$(r + I)(s + I) = rs + I$$

Para analizar si el cociente es un anillo basta con probar los axiomas de anillos con las operaciones definidas anteriormente.

Teorema 1.4. *Sea A un anillo conmutativo e I un ideal de A con $I \neq A$. El anillo cociente A/I es un dominio entero si y solo si I es un ideal primo de A.*

Demostración 1.7. Sea A/I un dominio entero, queremos demostrar que I es ideal primo de A.
Sean $a \in A$ y $b \in A$ tales que $ab \in I$, y además $(a+I)$; $(b+I) \in A/I$ entonces:

$$(a+I)(b+I) = ab + I = I$$

y como A/I es un dominio entero $a+I = I$ o $b+I = I$; esto implica que $a \in I$ o $b \in I$ con lo que I es un ideal primo de A.

Para el recíproco debemos demostrar que si I es un ideal primo de A, entonces A/I es un dominio entero. Supongamos que I es un ideal primo de A y sea

$$(a+I)(b+I) = I \tag{1.2.1}$$

para cualesquiera dos elementos $a+I$ y $b+I$ de A/I . Como

$$I = (a+I)(b+I) = ab + I \tag{1.2.2}$$

deducimos que $ab \in I$ y como I es primo $a \in I$ o $b \in I$, por tanto $a+I = I$ o $b+I = I$, lo que demuestra que A/I es un dominio entero.

Teorema 1.5. *Sea A un anillo conmutativo con uno. Si I es un ideal maximal de A entonces A/I es un cuerpo.*

Demostración 1.8. Supongamos que I es un ideal maximal en A. Se puede observar que si A es un anillo conmutativo con uno, entonces A/I también es un anillo conmutativo con uno cuando $I \neq A$, lo cual ocurre si I es maximal. Sea $(b+I) \in A/I$, con $b \notin I$, de modo que $b+I$ no es la identidad aditiva de A/I. Debemos mostrar que $b+I$ tiene inversso multiplicativo en A/I. Sea

$$N = \{ab + i \ \ / \ \ a \in A, \ \ i \in I\}$$

Entnonces, $\langle N, + \rangle$ es un grupo, pues

$$(a_1 b + i_1) + (a_2 b + i_2) = (a_1 + a_2)b + (i_1 + i_2),$$

y, claramente, lo ultimo está en N, además,

$$0 = 0b + 0 \qquad \text{y} \qquad -(ab + i) = (-a)b + (-i)$$

Ahora,

$$a_1(ab + i) = (a_1 a)b + a_1 i$$

muestra que $a_1(ab+i) \in N$ para $a_1 \in A$ y, como A es un anillo conmutativo, tambien $(ab+i)a_1 \in N$. Así, N es un ideal. Pero,

$$b = 1b + 0$$

muestra que $b \in N$ y para $i \in I$, y

$$i = 0b + i$$

muestra que $I \subseteq N$. De aquí, N es un ideal de A que contiene propiamente a I, pues $b \in N$ y $b \notin I$. Como I es maximal, debemos tener $N = A$. En particular, $1 \in N$. Entonces, por definición de N, existe $c \in A$ y $i \in I$ tal que $1 = cb + i$. Por lo tanto,

$$1 + I = cb + I = (c + I)(b + I),$$

de modo que $c + I$ es un inverso multiplicativo de $(b + I)$, como se quería demostrar.

1.2.2 Homomorfismo de anillos

El homomorfismo de anillos es similar al homomofismo de grupos.

Definición 1.13. *Una transformación ϕ de un anillo A en un anillo A' es un* ***homomorfismo*** *si cumple con*

$$\phi(a+b) = \phi(a) + \phi(b) \tag{1.2.3}$$

$$\phi(ab) = \phi(a)\phi(b) \tag{1.2.4}$$

para todos los elementos $a, b \in A$.

Teorema 1.6. *Si I es un ideal de un anillo A, entonces la transformación canónica $\gamma : A \to A/I$ dada por $\gamma(a) = a + I$ para $a \in A$ es un homomorfismo.*

Demostración 1.9. Para la condición 2.9 podemos realizar lo siguiente

$$\gamma(a+b) = (a+b) + I = (a+b) + I + I = (a+I) + (b+I) = \gamma(a) + \gamma(b)$$

pues los ideales son subanillos. Para la condición 2.10 realizamos lo siguiente

$$\gamma(ab) = ab + I = (a+I)(b+I) = \gamma(a)\gamma(b)$$

pues la multiplicación de clases está bien definida.

Ejemplo 1.2.9. *Sea R y R' dos anillos arbitrarios y definamos $\phi(a) = 0$ para todo $a \in R$. ϕ es trivialmente un homorfismo.*

Definición 1.14. *El* ***kernel o núcleo*** *de un homomorfismo ϕ de un anillo A en un anillo A' es el conjunto de todos los elementos de A cuya imagen es la identidad aditiva (o el cero) de A' bajo ϕ.*

1.2.3 Anillo de polinomio

Al conjunto de todos los polinomios $A[x]$ con variable x y coeficientes en el anillo A es un anillo bajo la suma y la multiplicación polinomial. Definimos los polinomios con coeficientes en un anillo A como la suma formal finita

$$\sum_{i=0}^{n} a_i x^i = a_1 x + a_2 x^2 + a_3 x^3 + ... + a_n x^n$$

donde $a_i \in A$ para $i = 1, 2, 3..., n$ y $n \in \mathbb{N}$.

La suma de polinomios es de forma trivial sumando los términos semejantes. Sea $m > n$

$$\sum_{i=0}^{n} a_i x^i + \sum_{j=0}^{m} b_j x^j = \sum_{i=0}^{n} (a_i + b_i) x^i + \sum_{j=n+1}^{m} b_j x^j$$

El producto de polinomios está definido como:

$$\left(\sum_{i=0}^{n} a_i x^i = a_1 x + a_2 x^2 + ... + a_n x^n \right) \cdot \left(\sum_{j=0}^{m} b_j x^j = b_1 x + b_2 x^2 + ... + b_m x^m \right)$$

$$= \sum_{i=0}^{n+m} c_i x^i$$

donde

$$c_i = \sum_{i+j=m+n}^{n+m} a_i b^j = a_0 \cdot b_{n+m} + a_1 \cdot b_{n+m-1} + a_2 \cdot b_{n+m-2} ... + a_{n+m} \cdot b_0$$

Teorema 1.7. *Sea $\mathbb{K}$ un cuerpo y $P(x)$ y $Q(x)$ dos polinomios de $\mathbb{K}[x]$, con $Q(x) \neq 0$; existen dos polinomios $S(x)$ y $R(x)$ también en el anillo $\mathbb{K}[x]$ tales que $P(x) = S(x)Q(x) + R(x)$ y $R(x) = 0$ ó $gr(R) < gr(Q)$.*

Demostración 1.10. Supongamos que $P(x) = a_m x^m + ... + a_0$ y $Q(x) = b_n x^n + ... + b_0$. Si $grP < grQ$ basta tomar $S(x) = 0$ y $R(x) = P(x)$; por lo tanto podemos suponer que $m \geq n$. Al ser $\mathbb{K}$ un cuerpo, b_n tiene un inverso multiplicativo que escribiremos b_n^{-1}, entonces

$$P(x) = (a_m b_n^{-1}) x^{m-n} Q(x) + [P(x) - (a_m b_n^{-1}) x^{m-n} Q(x) = (a_m b_n^{-1} x^{m-n} Q(x) + R'$$

Ahora bien

$$R'(x) = (a_m x^m + a_{m-1} x^{m-1} + ...) - (a_m b_n^{-1}) x^{m-n} (b_n x^n + ...)$$

$$= a_m x^m - a^m x^m + a_{m-1}x^{m-1} + ... = a_{m-1}x^{m-1} + ...$$

y $gr(R') \leq m-1 < gr(P)$. Si $R' = 0$ o $gr(R') < gr(Q)$, el teorema queda probado. Si por el contrario, $R' = c_p x^p + c_{p-1}x^{p-1} + ...$, con $p \geq n$, escribimos

$$P(x) = [(a_m b_n^{-1})x^{m-n} + (c_p b_n^{-1})x^{p-n}]Q(x) + [R'(x) - (c_p b_n^{-1})x^{p-n}Q(x)]$$

$$= c'(x)Q(x) + R''(x)$$

Con $gr(R'') < gr(R')$. es obvio que este proceso nos permite llegar en a lo sumo $m-n+1$ pasos a la descomposición $P(x) = S(x)Q(x) + R(x)$ deseada.

A continuación estudiaremos lo que comúnmente se conoce como **Resolución de una ecuación polinomial** donde hay dados $\mathbb{K}$ y $\mathbb{F}$ con la particularidad de que $\mathbb{K}$ es subcuerpo de $\mathbb{F}$. El siguiente teorema asegura la existencia de un homomorfismo importante de $\mathbb{K}[x]$ en $\mathbb{F}$.

Teorema 1.8 (Homomorfismo de evaluación)**.** *Sea $\mathbb{K}$ un subcuerpo de un cuerpo $\mathbb{F}$, sea α cualquier elemento de $\mathbb{F}$ y x una indeterminada. La transformación $\phi_\alpha : \mathbb{K}[x] \to \mathbb{F}$ definida por*

$$\phi_\alpha(a_0 + a_1 x + ... + a_n x^n) = a_0 + ... + a_n \alpha^n$$

para $(a_0 + a_1 x + ... + a_n x^n) \in \mathbb{K}[x]$ es un homomorfismo de $\mathbb{K}[x]$ en $\mathbb{F}$. Además $\phi_\alpha(x) = \alpha$ y ϕ_α transforma, de manera isomorfa, a $\mathbb{K}$, mediante la transformación idéntica , esto es $\phi_\alpha a = a$ para $a \in \mathbb{K}$. El homomorfismo ϕ_α es la evaluación en α.

Demostración 1.11. Si $f(x) = a_0 + a_1 x + ... + a_n x^n$, $g(x) = b_0 + b_1 x + ... + b_n x^n$, y $f(x) + g(x) = h(x) = c_0 + c_1 x + ... + c_n x^n$, entonces

$$\phi_\alpha(f(x) + g(x)) = \phi_\alpha(h(x)) = c_0 + c_1\alpha + ... + c_n\alpha^n$$

Mientras que

$$\phi_\alpha(f(x) + \phi_\alpha(g(x))) = (a_0 + a_1\alpha + ... + a_n\alpha^n) + (b_0 + b_1\alpha + ... + b_n\alpha^n)$$

Como por definición de suma polinomial tenemos que $c_i = a_i + b_i$ vemos que

$$\phi_\alpha(f(x) + g(x)) = \phi_\alpha(f(x)) + \phi_\alpha(g(x))$$

Pasando a la multiplicación, vemos que

$$f(x)g(x) = d_0 + d_1 x + ... + d_s x^s$$

Entonces

$$\phi_\alpha(f(x)g(x)) = d_0 + d_1\alpha + ... + d_s\alpha^s$$

Mientras que

$$[\phi_\alpha(f(x))][\phi_\alpha(g(x))] = (a_0 + a_1\alpha + ... + a_n\alpha^n)(b_0 + b_1\alpha + ... + b_n\alpha^n)$$

como por definición de multiplicación polinomial,

$$d_j = \sum_{i+j=n+n}^{n+n} a_i bj$$

vemos que

$$\phi_\alpha(f(x)g(x)) = [\phi_\alpha(f(x))][\phi_\alpha(g(x))]$$

Así, ϕ_α es un homomorfismo.

La definición de ϕ_α aplicada a una constante polinomial $a \in \mathbb{F}[x]$, donde $a \in \mathbb{F}$, da $\phi_\alpha a = a$, de modo que ϕ_α transforma a $\mathbb{K}$ de manera isomorfa, mediante la transformación identidad. De nuevo, por definición de ϕ_α tenemos $\phi_\alpha(x) = \phi_\alpha(1x) = 1\alpha = \alpha$.

Definición 1.15. *Sea $\mathbb{K}$ un subcuerpo de $\mathbb{F}$ y sea α un elemento de $\mathbb{K}$. Sea $f(x) = a_0 + a_1x + ... + a_nx^n$ en $\mathbb{K}[x]$ y sea $\phi_\alpha : \mathbb{K}[x] \to \mathbb{F}$ el homomorfismo de evaluación. Denotaremos por $f(\alpha)$*

$$\phi_\alpha(f(x)) = f(\alpha) = a_0 + a_1\alpha + ... + a_n\alpha^n$$

Si $f(\alpha) = 0$, entonces α es un cero de $f(x)$

1.3 Cuerpo

Definición 1.16. *Un cuerpo $\mathbb{K}$ es un conjunto dotado de dos operaciones binarias $+$ y $\cdot$ que llamaremos suma y producto, definidas en $\mathbb{K}$ tales que se satisfacen los siguientes axiomas:*

1. $(\mathbb{K}, +)$ es un grupo abeliano.
2. $\mathbb{K}^*$ es un grupo abeliano.
3. El producto es distributivo sobre la suma.

En otras palabras y utilizando todos los contenidos tratados en la sección anterior, podemos definir un cuerpo $\mathbb{K}$ como un anillo de división conmutativo.

Teorema 1.9. *Si A es un anillo con uno y tiene características $n > 1$, entonces A contiene un anillo isomorfo a $\mathbb{Z}_n$. Si A tiene características 0, entonces A contiene un subanillo isomorfo a $\mathbb{Z}$.*

Demostración 1.12. Es fácil que la demostración $\phi : \mathbb{Z} \longrightarrow \mathbb{R}$ dada por $\phi(n) = n \cdot 1$ donde $n \in \mathbb{Z}$ es un homomorfismo. El núcleo debe ser el ideal de $\mathbb{Z}$. Todos los ideales de $\mathbb{Z}$ son de la forma $m\mathbb{Z}$ para algún $m \in \mathbb{Z}$

Teorema 1.10. *Un cuerpo $\mathbb{K}$ que tiene caracteristicas p (con p un número primo) contiene un subcuerpo isomorfo a $\mathbb{Z}_p$.*

Demostración 1.13. Si la característica de A no es 0, entonces el teorema anterior muestra que contiene un subanillo isomorfo a $\mathbb{Z}_n$, entonces n debe ser un primo, pues si no A tendría divisores de 0.

1.3.1 Cuerpos finitos

Un cuerpo finito es aquel cuerpo definido en un conjunto finito de elementos.

Un ejemplo muy utilizado es el conjunto $\mathbb{F}_p$ (con un primo p), pues este conjunto forma un cuerpo con p elementos.

Definición 1.17. *Sean $\mathbb{E}$ y $\mathbb{F}$ cuerpos, $\mathbb{F} \leq \mathbb{E}$. Un elemento $\alpha \in \mathbb{E}$ se dice que es **algebraico sobre** $\mathbb{F}$ si es cero de algún polinomio no nulo de $\mathbb{F}[x]$. En caso contrario se dice que el elemento α es **trascendental sobre** $\mathbb{F}$.*

Ejemplo 1.3.1. *$\mathbb{Q} \leq \mathbb{C}$ y $\sqrt{2}$ e i son algebraicos sobre $\mathbb{Q}$ ya que son ceros, respectivamente, de $x^2 - 2$ y $x^2 + 1$.*

Definición 1.18. *Supongamos que $\mathbb{E}$ es una extensión de un cuerpo $\mathbb{F}$. Diremos que $\mathbb{E}$ es una extensión algebraica si todo elemento de $\mathbb{E}$ es algebraico sobre $\mathbb{F}$.*

Ejemplo 1.3.2. *$\mathbb{C}$ es una extensión algebraica de $\mathbb{R}$. Si $a + bi \in \mathbb{C}$, entonces $(a + bi)^2 = a^2 - b^2 + 2abi$, luego $(a + bi)^2 - 2a(a + bi) + a^2 + b^2 = 0$, lo que quiere decir que $a + bi$ es raíz de $x^2 - 2ax + \left(a^2 + b^2\right) \in \mathbb{R}[x]$.*

Teorema 1.11. *Sea $\mathbb{E}$ una extensión de un cuerpo $\mathbb{F}$, y sea $\alpha \in \mathbb{F}$ un elemento algebraico sobre $\mathbb{F}$. Entonces todo elemento β de $\mathbb{F}(\alpha)$ es algebraico sobre $\mathbb{F}$, y $deg(\beta, \mathbb{F}) \leq deg(\alpha, \mathbb{F})$.*

Demostración 1.14. Sabemos que si $deg(\alpha, \mathbb{F}) = n+1$, entonces $\{1, \alpha, ..., \alpha^n\}$ es una base de $\mathbb{F}(\alpha)$ como $\mathbb{F} - espacio\ vectorial$. Consideremos ahora un elemento $\beta \in \mathbb{F}(\alpha)$. El conjunto $\left\{1, \beta, ..., \beta^n, \beta^{n+1}\right\} \subseteq \mathbb{F}(\alpha)$ es linealmente dependiente ($\mathbb{F}(\alpha)$ tiene dimensión $n + 1$ como espacio vectorial sobre $\mathbb{F}$), luego existen $b_0 + b_1\beta + ... + b_{n+1}\beta^{n+1} \in \mathbb{F}$, no todos nulos, tales que $b_0 + b_1\beta + ... + b_{n+1}\beta^{n+1} = 0$. Esto quiere decir que el polinomio $f(x) = b_0 + b_1x + ... + b_{n+1}x^{n+1} \in \mathbb{F}[x]$ es no trivial y tiene a β como raíz, por lo que $deg(\beta, \mathbb{F}) \leq n + 1 = deg(\alpha, \mathbb{F})$.

Definición 1.19. *Sea $\mathbb{F} \leq \mathbb{E}$ una extensión de cuerpos. Si la dimensión de $\mathbb{E}$ como espacio vectorial sobre $\mathbb{F}$ es finita, digamos n, entonces diremos que $\mathbb{E}$ es una* ***extensión finita de grado n sobre*** *$\mathbb{F}$.*

Teorema 1.12. *Sea $\mathbb{F}$ una extensión finita de grado n de un cuerpo finto $\mathbb{K}$. Si $\mathbb{K}$ tiene q elementos, entonces $\mathbb{F}$ tiene q^n elementos.*

Demostración 1.15. Sea $\alpha_1, \alpha_2, ..., \alpha_n$ una base para $\mathbb{F}$ sobre $\mathbb{K}$. Entonces, toda $\beta \in \mathbb{F}$ puede escribirse de manera única como:

$$\beta = k_1\alpha_1 + ... + k_n\alpha_n$$

para $K_i \in \mathbb{K}$. Como cada K_i puede ser algun q de $\mathbb{K}$, entonces el número total de dichas combinaciones lineales distintas de las α_2 es q^n. Entonces $\mathbb{K}$ debe tener q^n elementos.

Corolario 1.2. *Si un cuerpo finito $\mathbb{K}$ es de características p, entonces contiene q^n elementos, siendo p la característica y n algún número natural.*

Demostración 1.16. Todo cuerpo finito $\mathbb{K}$ tiene características p (con p primo), por lo que existe un subcuerpo $\mathbb{S}$ isomorfo a $\mathbb{Z}_p$, por lo que $\mathbb{S}$ contiene p elementos. Por el teorema anterior, $\mathbb{K}$ (puesto que es una extensión de $\mathbb{S}$ existe un n tal que sea el grado de esa extensión) contiene q^n elementos.

Lema 1.5. *Si $\mathbb{K}$ es un cuerpo finito de características p, entonces $x^{p^n} - x$ tiene q^n ceros distintos en el cuerpo de descomposición $\mathbb{K} \leq \overline{\mathbb{K}}$ sobre $\mathbb{K}$. (Entiendase $\overline{\mathbb{K}}$ como la* ***clausura algebraica de*** *$\mathbb{K}$).*

Demostración 1.17. Sea $\mathbb{K}$ un cuerpo finito de características p y sea $\mathbb{F}$ el cuerpo de descomposición en $\overline{\mathbb{K}}$ del polinomio $x^{p^n} - x$ sobre $\mathbb{K}$. Se pretende mostrar que el polinomio recién mencionado contiene q^n ceros distintos en $\mathbb{F}$. Es evidente que 0 es un cero de $x^{p^n} - x$ de multipicidad 1. Ahora bien, supongamos que $\alpha \neq 0$ es un cero de $x^{p^n} - x$ lo que es equivalente a decir que es un cero de $f(x) = x^{p^{n-1}} - 1$. Entonces, $x - \alpha$ es un factor de $f(x)$ en $\mathbb{F}(x)$ y mediante división podemos obtener:

$$\frac{f(x)}{(x-\alpha)} = g(x) = x^{p^n-2} + \alpha x^{p^n-3} + \cdots + \alpha^{p^n-3}x + \alpha^{p^n-2}$$

Ahora. $g(x)$ tiene $p^n - 1$ sumandos y en $g(\alpha)$ cada sumando es

$$\alpha^{p^n-2} = \frac{\alpha^{p^n-1}}{\alpha} = \frac{1}{\alpha}$$

$$g(\alpha) = [(p^n - 1) \cdot 1]\frac{1}{\alpha} = -\frac{1}{\alpha}$$

Esto ya que estamos en un cuerpo de características p. Por tanto $g(\alpha) \neq 0$. De modo que α es un cero de $f(x)$ de multiplicidad 1.

Teorema 1.13. *Si $\mathbb{K}$ es un cuerpo finito, entonces $\mathbb{K}^*$ es un cuerpo ciclíco.*

Demostración 1.18. Como $\mathbb{K}^*$ es un cuerpo abeliano de orden $q-1$ entonces se puede representar como

$$\mathbb{K}^* \simeq \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times ... \times \mathbb{Z}_{d_n}$$

de modo que $d_1 > 1$ y $d_i | d_{i+1}$ para $1 < i \leq s$ .Por Teorema fundamental de grupos abelianos finitamente generados (Factores invariantes).

Un elemento $a \in \mathbb{Z}_{d_1} \cdot ... \cdot \mathbb{Z}_{d_s}$ puede tener orden r que divide a un d_i,en cualquier caso, $r | d_s$. Entonces para todo $a \in \mathbb{K}^*$ se cumple

$$a^{d_s} - 1 = 0$$

El polinomio $a^{d_s} - 1 = 0$ sobre $\mathbb{K}$ puede tener a lo mas d_s raíces, por lo tanto

$$|\mathbb{K}^*| = q - 1 \leq d_s$$

y puesto que $d_s || \mathbb{K}^*|$ se tiene que $d_s \leq ||\mathbb{K}^*|$ entonces

$$|\mathbb{K}^*| = q - 1 = d_s$$

por lo tanto $\mathbb{K}^* \simeq \mathbb{Z}_{d_s}$, lo que prueba que $\mathbb{K}^*$ es cíclico.

Por último, definiremos residuo cuadrático pues será de utilidad en el capítulo 4: Test e implementaciones.

Definición 1.20. *Para todo a y p un primo impar tal que $(a, p) = 1$, recibe el nombre de residuo cuadrático módulo p si la congruencia $x^2 \equiv a (mód\ p)$ tiene una solución. Si no tiene una solución, entonces a es un residuo no cuadrático.*

Ejemplo 1.3.3. *Si tomamos el primo $p = 13$, se tiene que*

$$1^2 = 12^2 \equiv 1 (mód\ 13)$$
$$2^2 = 11^2 \equiv 4 (mód\ 13)$$
$$3^2 = 10^2 \equiv 9 (mód\ 13)$$
$$4^2 = 9^2 \equiv 3 (mód\ 13)$$
$$5^2 = 8^2 \equiv 12 (mód\ 13)$$
$$6^2 = 7^2 \equiv 10 (mód\ 13)$$

Por lo tanto, 1,3,4,9,10 y 12 son residuos cuadráticos módulo 13 y 2,5,6,7,8 y 11 son residuos no cuadráticos.

1.4 Espacio proyectivo y punto en el infinito

Es sabido que dos rectas se intersecan en el infinito. El ***Espacio proyectivo*** nos permite dar un sentido lógico a esta afirmación, además nos permite interpretar lo que es punto en el infinito de una curva elíptica.
Dado un cuerpo $\mathbb{K}$, el espacio protectivo $P_{\mathbb{K}^2}$ duo-dimensional sobre $\mathbb{K}$ es dado por las clases de equivalencia triples (x, y, z) con $x, y, z \in \mathbb{K}$ y al menos una x, y, z no cero.

Definición 1.21. *Las dos triples (x_1, y_1, z_1) y (x_2, y_2, z_2) se dicen equivalentes si existe un elemento no cero $\lambda \in \mathbb{K}$ tal que*

$$(x_1, y_1, z_1) = (\lambda x_2, \lambda y_2, \lambda z_2)$$

que escribiremos como $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$. Las clases de equivalencia de un triple solo dependen de los valores de x a y a z. Por lo tanto, la clase de equivalencia (x, y, z) es denotada por $(x : y : z)$.

Definición 1.22. *Si $(x : y : z)$ es un punto con $z \neq 0$, entonces $(x : y : z) = (x/z : y/z : 1)$ y este es un punto finito en $P^2_{\mathbb{K}}$. Entonces si $z = 0$ dividir por z debe ser visto como ∞ en la coordenada x o y, por ello el punto $(x : y : 0)$ es llamado punto en el infinito de $P^2_{\mathbb{K}}$.*

Definición 1.23. *El plano afín duo-dimensional sobre $\mathbb{K}$ es denotado por*

$$A^2_{\mathbb{K}} = \{(x, y) \in \mathbb{K} \times \mathbb{K}\}$$

Nosotros tenemos una inclusión

$$A^2_{\mathbb{K}} \hookrightarrow P^2_{\mathbb{K}}$$

dada por

$$(x, y) \mapsto (x : y : 1)$$

De esta manera, el plano afín se identifica con los puntos finitos en $P^2_{\mathbb{K}}$. La adición de los puntos en la infinidad para obtener $P^2_{\mathbb{K}}$ puede verse como una forma de compactificar el plano.

Definición 1.24. *Un polinomio P se dice **Homogéneo** de grado n si*

$$P(\lambda x, \lambda y, \lambda z) = \lambda^n P(x, y, z) para\ todo \lambda \in \mathbb{K}$$

Definición 1.25. *Si $f(x, y)$ es un polinomio de valores de x e y, nosotros podremos homogeneizarlo insertando las potencias apropiadas de z.*

Teorema 1.14. *La intersección de dos rectas pararelas en el espacio proyectivo es el punto en el infinito* $(1 : m : 0)$.

Demostración 1.19. Nosotros tomaremos dos rectas de la forma

$$y = mx + b_1 \qquad y = mx + b_2$$

Estas dos rectas son oblicuas paralelas con $b_1 \neq b_2$. Ellas tienen sus formas homogéneas

$$y = mx + b_1 z \qquad y = mx + b_2 z$$

Al buscar la intersección de ambas rectas obtenemos los siguientes resultados

$$z = 0 \quad \text{e} \quad y = mx$$

Por definición .... no podemos tener x, y, z todos cero, por lo cual obtenemos un $m \neq 0$. Por lo tanto nosotros podemos reescribir realizando el cociente por x y finalmente obteniendo la intersección de ambas rectas

$$(x : mx : 0) = (1 : m : o)$$

CAPÍTULO 2

Test de primalidad

Supongamos que n es un entero de varios cientos de dígitos decimales. Por lo general, es fácil saber con algo de certeza si n es primo o compuesto. Pero supongamos que realmente queremos demostrar que nuestra respuesta es correcta. Si n es compuesto, entonces usualmente conocemos un factor no trivial o n falla una prueba de pseudoprimidad .

Por lo tanto, cuando n es compuesto, generalmente es fácil probarlo, pero si n es primo, la situación es más difícil. Decir que n pasó varias pruebas de pseudoprimalidad indica que n es probablemente primo, pero no prueba que n sea verdaderamente primo.

Cohen y Lenstra desarrollaron métodos con sumas de Jacobi que funcionan bien para números primos de unos pocos cientos de dígitos. Sin embargo, para números primos de mil dígitos o más, el método más popular actualmente en uso involucra curvas elípticas.

En este capítulo revisaremos de manera breve los test de primalidad más relevantes para nuestro estudio, pero no sin antes mencionar por qué son tan importantes y atractivos los números primos.

2.1 Números primos

A lo largo de la historia de las matemáticas los números primos han ido dejando un extenso rastro de conjeturas. “Su estudio, ha generado nuevas teorías, nuevos paradigmas, nuevos hitos que han marcado un antes y un después, y todo apunta a que esto seguirá siendo así durante mucho tiempo” dice Enrique Gracián (2010). Para saber lo que es un número primo basta con conocer un

sistema de numeración y las cuatro operaciones fundamentales. Sin embargo, han sido y siguen siendo uno de los retos más fabulosos de la historia de la ciencia. Ahora bien ¿Cuándo un número es primo? Se dice que un número es primo cuando sólo es divisible por sí mismo y por la unidad.

Es frecuente referirse a los números primos como a los "ladrillos" de las matemáticas, puesto que son elementos primigenios a partir de los cuales se genera algo, en este caso los números naturales (Enrique Gracián,2010) . La palabra "primo", que proviene del latín primus, quiere decir "primero" y alude al concepto de "primario", "primitivo", en el sentido de origen, ya que todos los números pueden obtenerse a partir de ellos. Esto es lo que llamamos El teorema fundamental de la aritmética. Sin embargo, algo análogo para los números primos y sin ambigüedades, no existe. Los números primos aparecen como un conjunto caótico, y se distribuyen de manera aparentemente aleatoria por la serie de los números naturales.

Esto fue lo primero que llamó la atención a los antiguos matemáticos en relación a los números primos: la ausencia de pautas en cuanto a su aparición en la sucesión de los números naturales. Y no sólo eso, sino que resulta que tampoco tienen un comportamiento claro por lo que respecta a su ausencia, es decir, la manera en que dejan de aparecer. Por consiguiente, pueden estar relativamente juntos o, por el contrario, distanciarse muchísimo. Aun así, sabemos que el teorema de Euclides garantiza que hay infinitos números primos y que, por muy larga que sea una serie de números compuestos, en algún momento volverá a aparecer un número primo.

A la fecha, el número primo con mayor cantidad de dígitos que se ha encontrado es el primo de Mersenne $2^{82589933} - 1$ con casi 25 millones de dígitos. Fue hallado por GIMPS (Gran búsqueda de números primos de Mersenne por Internet) un proyecto de computación que utiliza programas gratuitos con el fin de buscar números primos de Mersenne.

2.2 Test de primalidad

Determinar si un cierto número es primo o compuesto se denomina problema de primalidad. Y los métodos que dan con la solución son algoritmos conocidos como test de primalidad. Existen dos tipos de test, lo deterministas y los probabilísticos. Los test deterministas son capaces de afirmar con absoluta certeza la primalidad de un número dado. En cambio, los test probabilísticos sólo nos

indican qué tan probable es que dicho número sea primo, sin ningún tipo de garantía matemática (Eugenia Bernaschini, 2017). Actualmente, su interés de estudio es debido a la criptografía. Los métodos criptográficos actuales usan números primos de muchas cifras como parte fundamental del proceso de encriptación. El mayor problema es que la seguridad del método se diluye cuando elegimos un número que creemos es primo cuando sin embargo no lo es, por lo que es fundamental tener algoritmos rápidos y eficientes que certifiquen la primalidad (Cruz Borges, 2005).

Entre los test de primalidad, se encuentran certificados de primalidad y composición clásicos, tales como el test indeterminista de compositud, así como también están otros algoritmos importantes y didácticos.

El algoritmo de Miller-Rabin, que es uno de los mejores y más rápidos test de primalidad, tanto es así que es el test estándar en prácticamente todos los paquetes informáticos. El test se basa en la siguiente propiedad.

Teorema 2.1. *Sea n un primo impar y sea $n-1 = 2^s r$ donde r es impar. Sea a cualquier entero tal que $mcd(a,n) = 1$. Entonces $a^r \equiv 1 (mód\ n)$ o $a^{2jr} \equiv -1 (mód\ n)$ para algún j, $0 \leq j \leq s-1$.*

Demostración 2.1. Si $a^r \equiv 1$ mód n Listo!!
Si $a^r \not\equiv 1$ mód n prodeceremos por contradicción.
Como la ecuación $x^2 \equiv 1$ mód n tiene soluciones 1 y -1 tenemos que si $a^{2r} \equiv 1$ mód n entonces $a^r \equiv -1$ mód n Listo!!
Si $a^{2r} \not\equiv 1$ mód n y $a^{4r} \equiv 1$ mód n entonces $a^{2r} \equiv -1$ mód n. Listo!!
Repitiendo el argumento si $a^{4r} \not\equiv 1$ mód n y $a^{8r} \equiv 1$ mód n Listo !! si ninguno de los $a^r, a^{2r}, a^{4r}, ..., a^{2^{s-2}}$ es equivalente a 1 módulo n entonces $a^{2^{s-1}} \not\equiv 1$ mód n y como $a^{2^s r} \equiv 1$ mód n entonces $a^{2^{s-1} r} \equiv -1$ mód n lo que prueba lo deseado.

Definición 2.1. *Sea n un número entero compuesto impar y sea $n-1 = 2^s r$ donde r es impar. Sea a un entero en el intervalo $[1, n-1]$.*

a) Si $a^r \not\equiv 1 (mód\ n)$ y si $a^{2jr} \not\equiv -1 (mód\ n)$ para todo j, $0 \leq j \leq s-1$, entonces a es denominado un testigo fuerte para n.

b)De otra manera, esto es, si $a^r \equiv 1 (mód\ n)$ o $a^{2jr} \equiv -1 (mód\ n)$ para algún j, $0 \leq j \leq s-1$, entonces se dice que n es un pseudónimo fuerte para la base a.(Quiere decir, n actúa como un primo que satisface el Teorema 2.2 para la base particular a). El número entero a se llama mentiroso fuerte para n.

Teorema 2.2. *Sea $n > 9$ un entero positivo impar compuesto. Escribamos $n-1 = 2^s r$ para algún exponente $s \geq 1$ y algún entero impar r. Sea*

$$B(n) = a \in (\mathbb{Z}/n\mathbb{Z})^x \mid a^r \equiv 1 (\textit{mód } n) \textit{para algún} 0 \geq < s$$

entonces

$$|B(n)| \geq \frac{\phi(n)}{4}$$

Demostración Para ver la demostración, se sugiere revisar [5]

2.2.1 Algoritmo de Miller-Rabin

Algoritmo 1: Test de primalidad probabilístico de Miller-Rabin.

Entrada : Un entero impar $n \geq 3$ y un parámetro de seguridad $t \geq 1$

Resultado: Una respuesta "primo probable" ó "compuesto" a la pregunta:"¿Es n un primo?"

```
1  Escribir n − 1 = 2^s r tal que r es impar;
2  para i de 1 a t hacer
3      Elegir al azar un entero a, 2 ≤ a ≤ n − 2;
4      Calcular y = a^r (mód n) ;
5      si y ≠ 1 e y ≠ n − 1 entonces
6          j ← 1;
7          mientras j ≤ s − 1 e y ≠ n − 1 hacer
8              Calcular el y ← y^2 (mód n) ;
9              si y = 1 entonces
10                 devuelve ("compuesto")
11             j ← j + 1;
12         si y ≠ n − 1 entonces
13             devuelve("compuesto")
14 Devuelve ("primo probable")
```

Al menos $\frac{3}{4}$ de todos los elementos en $[1, n-1]$ son testigos para n, cuando n es un número compuesto impar. La probabilidad de que el algoritmo falle para producir un testigo para n es $< \frac{1}{4}$, y por lo tanto si repetimos el algoritmo t veces independientemente, la probabilidad para que este falle es $< \frac{1}{4^t}$. si la respuesta de las t repeticiones del algoritmo no dan un testigo, solo podemos hacer una conjetura de que n es primo, con probabilidad mayor que $1 - \frac{1}{4^t}$. Por el uso de exponenciación modular, se tienen el tiempo de complejidad $O(M(n) \log n)$

Ejemplo 2.2.1. *Sea $n = 561$ probar si es primo.*

1. $561 - 1 = 560 = 2^4 \cdot 35$
2. *Escogemos* $a = 2$
3. *Calculamos* $y_0 = 2^{35} \equiv 263 \mod 561$
   - $y_1 \equiv y_0^2 \equiv 263^2 \equiv 166 \mod 561$
   - $y_2 \equiv y_1^2 \equiv 166^2 \equiv 67 \mod 561$
   - $y_3 \equiv y_2^2 \equiv 67^2 \equiv 1 \mod 561$

Por lo tanto 561 no es primo, es compuesto.

Finalmente, el algoritmo AKS es uno de los más importantes, pues es el primer algoritmo determinista que certifica la primalidad. Permite encontrar primos con más dígitos y que no pertenezcan a ninguna familia conocida con mayor facilidad, por lo que se dificulta la búsqueda de los mismos, por métodos de criptoanálisis más comunes.

2.2.2 Test de Pocklington-Lehmer

Pasamos ahora a considerar el problema práctico de probar rigurosamente que un número n es primo. Naturalmente, sólo tiene sentido hacer esta prueba cuando existe sospecha de que el número es primo; esto puede conseguirse usando el test de Miller-Rabin. La siguiente proposición nos servirá para desarrollar uno de los métodos más conocidos: el test de Pocklington-Lehmer.

Proposición 2.1. *Sea $n \geq 3$ un entero. Entonces n es primo si y sólo si existe un entero b que satisface*

$$b^{n-1} \equiv 1 (\textit{mód } n)$$
$$b^{\frac{(n-1)}{q}} \not\equiv 1 (\textit{mód } n)$$

Para cada divisor primo q de $n - 1$.

Demostración 2.2. Se deduce inmediatamente del hecho de que $\mathbb{Z}_n^*$ contiene un elemento de orden $n - 1$ si y sólo si n es primo.

Naturalmente, el inconveniente es que necesitamos conocer la factorización completa de $n - 1$ para poder aplicar este método. Pocklington demostró un resultado que permite aprovechar una factorización parcial de $n - 1$, descrita por Brillhart. El resultado de Pocklington es el siguiente:

Proposición 2.2. *Sea n un entero positivo y sea p un divisor primo de $n-1$. Supóngase que puede encontrarse un entero a_p tal que*

$$a_p^{n-1} \equiv 1 (mód\ n)$$

y, además,

$$mcd(a_p^{\frac{n-1}{p}} - 1, n) = 1$$

Entonces, si d es cualquier divisor de n, se tiene

$$d \equiv 1 (mód\ p^{a_p})$$

La idea de Lehmer es entonces la siguiente: supongamos ahora que se puede escribir $n-1 = F \cdot U$, donde F y U son primos entre sí, F está factorizado completamente y $F > \sqrt{n}$. Si para cada primo p que divide a F se puede entontrar un a_p que satisface las coondiciones de la proposición 2.2, entonces n es primo. Recíprocamente, si n es primo, entonces para cualquier factor primo p de $n-1$ se puede encontrar un a_p que satisface las condiciones de la proposición 2.2.

Demostración 2.3. Claramente es suficiente probar el resultado sólo cuando d es un divisor primo de n (ya que cualquier divisor de n es producto de divisores primos). Sea entonces d un divisor primo de n. Como $a_p^{n-1} \equiv 1 (\text{mód } n)$, a_p está en el grupo de las unidades módulo n y también es coprimo con n. Por lo tanto también es coprimo con d, y tenemos $a_p^{d-1} \equiv 1 (\text{mód } d)$. Por otro lado, de $mcd(a_p^{(n-1)/p} - 1, n) = 1$ vemos que $a_p^{(n-1)/p} \not\equiv 1 (\text{mód } d)$ (de otra manera d divide a $a_p^{(n-1)/p} - 1$ y a n, contradiciendo el *mcd*.

Sea e el orden multiplicativo de a_p módulo d, obtenemos que $e|d-1$ (ya que $a_p^{d-1} \equiv 1 (\text{mód } d)$), $e \nmid (n-1)/p$ (ya que $a_p^{(n-1)/p} \not\equiv 1 (\text{mód } d)$) y $e|n-1$ (ya que $a_p^{n-1} \equiv 1 (\text{mód } n)$ y d divide a n, además tenemos $a_p^{n-1} \equiv 1 (\text{mód } d)$)

Entonces $e|n-1$ y $e \nmid (n-1)/p$. Esto significa que si eliminamos solo un factor p de $n-1$, e ya no lo divide. A su vez, esto significa que todos los factores p de $n-1$ están en e también, y así $p^{a_p}|e$. Como también $e|d-1$, significa que $p^{a_p}|d-1$ y entonces $d \equiv 1 (\text{mód } p^{a_p})$, como deseamos.

Algoritmo 2: Test de primalidad Pocklington-Lehmer.

Entrada : n, n es impar, p es un primo divisor de $n-1$, $n-1 = F \cdot U$

Resultado: Una respuesta "primo" ó "compuesto" a la pregunta:"¿Es n un primo?"

1. Elegir un número natural a tal que $1 < a < n$
2. Si $a^{n-1} \not\equiv 1(\text{mód } n)$, devuelve("compuesto")
3. Si $mcd(a_p^{\frac{n-1}{p}} - 1, n) \neq 1$, devuelve("compuesto")
4. Devuelve ("primo")

Ejemplo 2.2.2. *Sea* $n = 11351$, $n - 1 = 2 \cdot 5^2 \cdot 227$
Escogemos $F = 227 \cdot 5^2$, *con lo que significa que* $U = 2$. *Ahora está claro que* $mcd(F, U) = 1$ *y* $F > \sqrt{n}$.

Encontramos un a_p *para cada factor primo* p *de* F. *Esto es tomando* $a_p = 5$.

$$a_p^{n-1} \equiv 5^{11350} \equiv 1(mod\ 11351)$$

$$mcd(a_p^{\frac{n-1}{p}} - 1, n) = mcd(5^{2 \cdot 5 \cdot 227} - 1, 11351) = 1$$

Así cumple las condiciones necesarias. Ahora escogemos $a_p = 7$ *(Raíz primitiva de 11351)*

$$a_p^{n-1} \equiv 7^{11350} \equiv 1(mod\ 11351)$$

$$mcd(a_p^{\frac{n-1}{p}} - 1, n) = mcd(7^{2 \cdot 25} - 1, 11351) = 1$$

Así que funciona para a, *por lo tanto* n *es primo.*

CAPÍTULO 3

Introducción a las Curvas elípticas

Durante las últimas décadas, las curvas elípticas han estado jugando cada vez un papel más importante tanto en la teoría de números como en campos relacionados con la criptografía. Paralelamente, desde la década de 1980, se han encontrado dos aplicaciones relacionadas de curvas elípticas, una de factorización y otra de prueba de primalidad, siendo este último el tema principal del presente trabajo.

La principal ventaja de las curvas elípticas radica en el hecho de que hay muchas curvas elípticas que modifican un número n, por lo que si una curva elíptica no funciona, se puede probar otra.

El objetivo de este capítulo es desarrollar teoría de curvas elípticas para comprender el test Goldwaiser-Killian que se trabajará más adelante.

3.1 Definición de una curva elíptica

3.1.1 Conceptos previos

Es necesario definir dos conceptos importantes que son necesarios para comprender el concepto de curva elíptica:

Definición 3.1. *Sea $\mathbb{K}$ un cuerpo y un polinomio no constante $f \in \mathbb{K}[x,y]$, entonces el conjunto $C_f(\mathbb{K}) = \{(x,y) \in \mathbb{K}^2 | f(x,y) = 0\}$ se denomina* ***Curva afín***

Definición 3.2. *Sea C una curva afín y $p = (a,b) \in C$ decimos que p es un punto singular de C si satisface:*

$$\frac{\delta f(p)}{\delta x} = \frac{\delta f(p)}{\delta y} = 0$$

Definición 3.3. *Una **Curva elíptica** sobre un cuerpo $\mathbb{K}$ es una curva algebraica sin puntos singulares y viene dada por una ecuación del tipo:*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_i \in \mathbb{K}$$

denominada ecuación general de Weierstrass.

Definición 3.4. *Dos curvas elípticas E_1 y E_2 definidas sobre un cuerpo $\mathbb{K}$ y dada por la ecuación de weierstrass.*

$$E_1 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
$$E_2 : y^2 + a'_1xy + a'_3y = x^3 + a'_2x^2 + a'_4x + a'_6$$

se dice que son isomorfas sobre $\mathbb{K}$ si existen $u, r, s, t \in \mathbb{K}$ con $u \neq 0$ tal que el cambio de variables lineal

$$(x, y) \longrightarrow (u^2x + r, u^3y + u^2sx + t)$$

transforme la ecuación E_1 en la ecuación E_2.
La ecuación general puede simplificarse mediante un cambio de variables, particularmente para los casos cuando las características del cuerpo es distinta de 2 y 3.

Definición 3.5. *Si las características $\mathbb{K}$ es distinta de 2 y 3, entonces el cambio de variables:*

$$(x, y) \longrightarrow (\frac{x - 3a_1^2 - 12a_2}{36}, \frac{y - 3a_1x}{216} - \frac{a_1^3 + 4a_1a_2 - 12a_3}{240})$$

transforma la curva E en la curva:

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

donde A y $B \in \mathbb{K}$ siendo el discriminante de esa curva $\triangle = -16(4a^3 + 27b^2)$, teniendo encuenta que $\triangle \neq 0$ asegura una curva no singular.

Esta forma más simplificada de la curva elíptica E es llamada ecuación reducida de weierstrass.
Si $E/\mathbb{K}$ es una curva elíptica sobre un cuerpo $\mathbb{K}$, denotaremos po $E(\mathbb{K})$ el conjunto de puntos $p = (x, y) \in \mathbb{K} \times \mathbb{K}$ que satisfacen la ecuación de la curva junto con el punto infinito de la curva ∞.

Las curvas elípticas en su forma reducida tienen una de estas formas

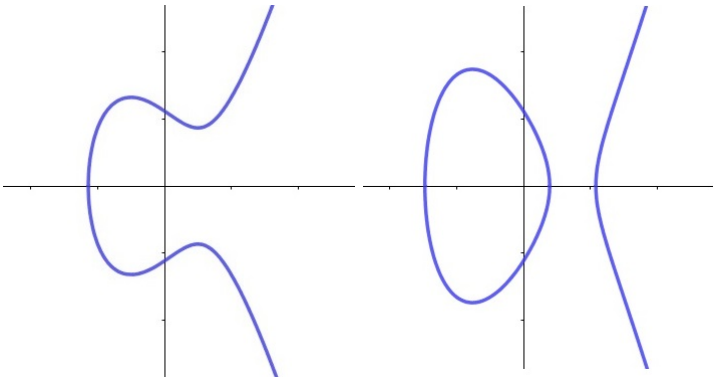

Figura 3.1: Curvas Elípticas

3.1.2 Suma elíptica

Comenzaremos definiendo el grupo de la operación adición como $\oplus$. Lo cual significa que dados dos puntos y sus coordenadas , $P = (x_1, y_1)$ y $Q = (x_2, y_2)$, nosotros obtendremos un tercer punto de la siguiente forma:

$$P \oplus Q = R$$

$$(x_1, y_1) \oplus (x_2, y_2) = (x_3, y_3)$$

A continuación se realizara una interpretación geométrica de la operacio para ayudar a visualizar correctamente, en este sentido se deberán distinguir dos casos: la adición de dos puntos distintos (denominada adición de puntos) y la adición de un punto a si mismo (denominado punto de duplicación).

Adición de puntos $P \oplus Q$ Es el caso del cálculo de $R = P \oplus Q$ y $P \neq Q$. La construción funciona de la diferente manera: Dibuje una recta que atraviese a P y Q obteniendo una tercera intersección entre la curva elíptica y la recta. Refleje dicho punto de intersección respecto al eje X. Este punto reflejado es por definición, el punto R. En la siguiente figura se puede observar la definición de una curva elíptica en los números reales.

Punto de duplicación $P \oplus P$ es el caso del cálculo de $P \oplus Q$, pero con $P = Q$. Entonces, nosotros podemos escribir $R = P \oplus P = 2P$. Necesitamos una ligera ayuda del cálculo diferencial para esta construcción. Se deberá dibujar la

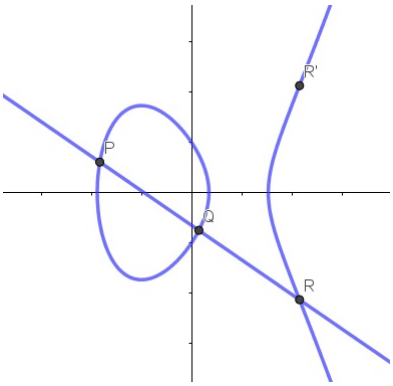

Figura 3.2: Adición de puntos

recta tangente a la curva en el punto P y obtener un segundo punto de intersección entre la curva y la recta. Reflejamos el segundo punto de intersección con repecto al eje X. Este punto reflejado resulta ser R.

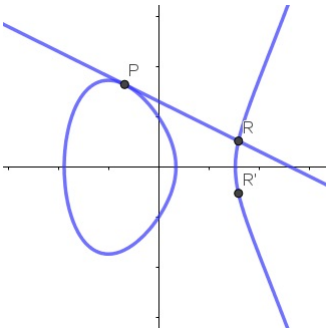

Figura 3.3: Punto de duplicación

Punto del infinito Un caso particular de suma que debemos prestar atención es para dados P, $P' \in E(\mathbb{K})$

$$P \oplus P' \text{ con } P' = refx[P]$$

La recta que pasa por P y P' resulta ser vertical de la forma $x = a$ y solo intersecta a la curva E en los puntos ya mencionados (observar figura 3.4). En estos casos se definirá el tercer punto d la intersección como 0 un punto del infinito sabiendo que $\infty \notin \mathbb{K} \times \mathbb{K}$

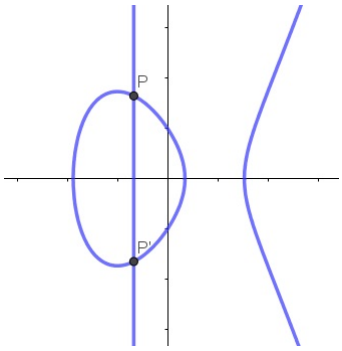

Figura 3.4: Punto del infinito

Teorema El punto en el infinito de una Curva Elíptica en el espacio proyectivo $(0:1:0)$.

Demostración Si observamos una curva elíptica E dado por $y^2 = x^3 + Ax + B$. Su versión homogénea será $y^2z = x^3 + Axz^2 + Bz^3$. El punto (x, y) en la curva original corresponde a los puntos $(x : y : 1)$ en la versión proyectiva. Al evaluar la curva en el punto en el infinito, con $z = 0$ y obtenemos $0 = x^3$. Por lo tanto $x = 0$, e y podremos obtener $(0 : y : 0) = (0 : 1 : 0)$ en el cual es el único punto en el infinito en la curva E.

Observación Como acabamos de trabajar $(0 : 1 : 0)$ pertenece a una recta vertical la cual inttersecta a E en ese punto de la infinidad. Además puesto que $(0 : 1 : 0) = (0 : -1 : 0)$, la parte "superior" y la parte "inferior" del eje y son iguales.

Suma infinita Dados P_1 y P_2

$$P \oplus P \quad \text{donde } P_2 = \infty$$

$$P \oplus \infty = P_1$$

Esto resulta evidente por definición de la suma elíptica.

Ejemplo 3.1.1. *Sea E la curva elíptica definida sobre los reales:*

$$E_{\mathbb{R}} : Y^2 = X^3 - 5X$$

Encontrar P+Q, con P(-1,2) y Q(0,0) puntos de la curva. Para determinar la adición de los puntos P y Q debemos trazar la recta que pase por estos dos

puntos, para así encontrar un tercer punto de intersección. El resultado de la suma será la reflexión del tercer punto con el eje X.

La recta que pasa por los puntos P(-1,2) y Q(0,0) es:

$$Y = -2X$$

Ahora para encontrar el tercer punto de intersección reemplazamos Y en la curva.

$$(-2X)^2 = X^3 - 5X$$

$$X^3 - 4X^2 - 5X = 0$$

$$X(X+1)(X-5) = 0$$

De aquí obtenemos el tercer valor, X=5, que reemplzamos en la ecuación de la curva para encontrar Y.

$$Y^2 = 5^2 - 5 \cdot 5$$

$$Y = \pm 10$$

Como la pendiente de la recta es negativa, la solución que nos sirve es -10, por lo tanto el tercer punto de intersección de la recta con la curva es (5,-10), que al reflejarlo con el eje X, para tener la solucion de la suma P+Q, nos da (5,10).

Teorema 3.1. *Dada una curva $E(\mathbb{K})$ de la forma $y^2 = x^3 + Ax + B$ con A, $B \in K$sde la suma elíptica de dos puntos $P = (x_1, y_1)$ y $Q = (x_2, y_2)$ puede ser decrita analíticamente como*

$$P + Q = (x_3, y_3), \quad P + Q \notin \infty$$

Donde:

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

Con $\lambda =$

$$\frac{y_1 - y_2}{x_1 - x_2} \ si\ x_1 \neq x_2$$

$$\frac{3x_1^2 + A}{2y_1} \ si\ x_1 = x_2 \ e\ y_1 = y_2 \neq 0$$

Demostración 3.1. dados $P(x_1, y_1)$ y $Q(x_2, y_2)$ dos puntos pertenecientes de a la curva E. En el caso que la recta sea de la forma $Y = \lambda X + v$ donde $v = y_1 - \lambda x_1$. Sustituyendo la recta en la curva E obtenemos

$$(\lambda X + v)^2 = X^3 + AX + B$$

$$X^3 - \lambda^2 X^2 + (A - 2\lambda v)X + (B - v^2) = 0$$

Sabiendo que x_1 y x_2 son raíces del polinomio cúbico. La tercera raíz sera x_3, por lo que los factores resultarán de la siguiente manera:

$$X^3 - \lambda^2 X^2 + (A - 2\lambda v)X + (B - v^2) = (X - x_1)(X - x_2)(X - x_3)$$

Si observamos detenidamente la igualdad podemos notar que deben cumplirse las siguientes igualdades:

$$-\lambda^2 = -x_1 - x_2 - x_3$$

lo que es equivalente a decir

$$x_3 = \lambda^2 - x_1 - x_2$$

verificando la primera igualdad. Así la coordenada Y de la tercera intersección de la recta con la curva E estará dada por $\lambda x_3 + v$ el cual mediante manipulación algebraica puede ser vista como $\lambda(x_3 - x_1) + y_1$. Realizando una reflexión respecto del eje X al punto finalmente obtenido tendremos que

$$y_3 = \lambda(x_1 - x_3) - y_1$$

obteniendo lo deseado. Cabe decir que el cálculo de λ como la pendiente de la recta corresponde a la simple aplicación de la pendiente de dos puntos o la pendiente de la recta tangente en un punto.

3.1.3 Estructuras en una curva elíptica

La operación suma de puntos de una curva elíptica cumple con los axiomas necesarios para que sea un grupo, pues:

- **Cerradura**: para cualquier P y $Q \in E$, $(P + Q) \in E$
- **Neutro**: $P + \infty = P$, $\forall\ P \in E$
- **Inverso**: dado $P \in E$ existe $P' \in E$ tal que $P + P' = \infty$
- **Asociatividad**: $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3), \forall\ P_1, P_2, P_3 \in E$
- **Conmutatividad**: $P_1 + P_2 = P_2 + P_1$

Lo que convierte a este grupo en abeliano.

Demostración 3.2. Analizando estos axiomas de forma geométrica, podemos ver que la existencia del elemento neutro es clara, pues es ∞, ya que la recta L que pasa por ∞ y un $P \in E$ es paralela al eje Y po lo que el tercer punto de intersección es el reflejo de P con respecto al eje X siendo así la suma del mismo P. De la misma forma se explica la existencia de inversos dentro del grupo. Además, como la suma está definida de tal forma que siempre obtengamos un punto de la curva, podemos afirmar que el grupo es cerrado.

El hecho de que la recta que pasa por P_1 y P_2 es la misma recta que pasa por P_2 y P_1, la conmutatividad es evidente.

3.2 Curvas elípticas sobre cuerpos finitos

Definimos una curva elíptica sobre el cuerpo finito $\mathbb{F}_p$

$$\mathrm{E} : Y^2 = X^3 + AX + B \text{ con } A, B \in \mathbb{F}_p$$

que satisfaga $4A^3 + 27B^2 \neq 0$

Definiremos el espacio de los puntos de la curva E como

$$\mathrm{E}(\mathbb{F}_p) = \{(x, y) : x, y \in \mathbb{F}_p \text{ satisface } y^2 = x^3 + Ax + B\} \cup \{\infty\}$$

Teorema 3.2. *Las operaciones sobre cuerpos finitos pueden definirse al igual que sobre un cuerpo cualquiera (nota: considerando la característica $p > 3$) mediante las siguientes formas*

$$x_3 = \lambda^2 - x_1 - x_2 \ mod\ p \qquad y_3 = \lambda(x_1 - x_3) - y_1 \ mod\ p$$

Donde λ :

$$\frac{y_1 - y_2}{x_1 - x_2} \ mod\ p \ , \ si\ x_1 \neq x_2 \ mod\ p$$

$$\frac{3x_1^2 + A}{2y_1} \ mod\ p \ , \ si\ x_1 = x_2 \ e\ y_1 = y_2 \neq 0 \ mod\ p$$

Ejemplo 3.2.1. *Sea la curva elíptica $E : y^2 = x^3 - 2x + 3$ sobre $\mathbb{F}_5$. Los puntos $(3, 2)$ y $(4, 3)$ pertenecen a $E(\mathbb{F}_5)$. Para encontrar la suma de los dos puntos utilizamos el teorema sabiendo que $x_1 \neq x_2$, entonces:*

$$\lambda = \frac{3 - 2}{4 - 3} = 1 \equiv 1 \ mod\ 5$$

$$x_3 = 1^2 - 3 - 4 = -6 \equiv -1 \equiv 4 \ mod\ 5$$

$$y_3 = 1(3 - 4) - 2 = -3 \equiv 2 \ mod\ 5$$

Por lo tanto, $(3, 2) + (4, 3) = (4, 2)$ *mod 5*

Teorema 3.3. ***Teorema de Hasse*** *dada una curva elíptica E sobre* $\mathbb{F}_p$

$$\#E(\mathbb{F}_p) = p + 1 - t_p \qquad \textit{satisfaciendo } |t_p| \leq 2\sqrt{p}$$

Demostración para ver la demostración del teorema, se sugiere revisar [12].

Ejemplo 3.2.2. *Sea E la curva* $y^2 = x^3 + x + 1$ *sobre* $\mathbb{F}_5$. *Probar* $|t_p| \leq 2\sqrt{5}$

x	$x^3 + x + 1$	y	puntos
0	1	± 1	(0,1) , (0,4)
1	3	-	-
2	1	± 1	(2,1) , (2,4)
3	1	± 1	(3,1) , (3,4)
4	4	± 2	(4,2) , (4,3)

Con los puntos obtenidos, más el ∞, *sabemos que* $\#E(\mathbb{F}_5) = 9$. *Luego*

$$9 = 5 + 1 - t_p$$

$$t_p = -3$$

Satisfaciendo $|-3| \leq 2\sqrt{5}$.

El teorema de Hasse se relaciona con el algoritmo de Schoof de conteo de puntos que se utilizará mas adelante.

3.2.1 La J-invariante

Sea una curva elíptica E definida por $y^2 = x^3 + Ax + B$ donde A y B son elementos de un cuerpo $\mathbb{K}$ que es de característica distinta de 2 y 3. Si tomamos

$$x_1 = \mu x \qquad y_1 = \mu^3 y$$

Con $\mu \in \bar{K}^*$ entonces obtenemos

$$y_1^2 = x_1^3 + A_1 x_1 + B_1$$

con $A_1 = \mu^4 A$ $B_1 = \mu^6 B$. La J-invariante de la curva E, queda definida por

$$j = i(E) = 1728 \frac{4A^3}{4A^3 + 27B^2}$$

Note que el denomidador es el negativo del discriminante por lo que es distinto de cero. Además el cambio de variables realizado deja a la j sin cambios. Lo contrario tambiés es verdad.

Teorema 3.4. *Sean* $y_1^2 = x_1^3 + A_1x_1 + B_1$ *y* $y_2^2 = x_2^3 + A_2x_2 + B_2$ *dos curvas elípticas con j-invariantes* j_1 *y* j_2 *respectivamente. Si* $j_1 = j_2$*, entonces existe un* $\mu \neq 0 \in \bar{K}$ *tal que*

$$A_2 = \mu^4 A_1 \qquad B_2 = \mu^6 B_1$$

La transformación

$$x_2 = \mu^2 x_1 \qquad y_2 = \mu^3 y_1$$

transforma una ecuación en la otra.

CAPÍTULO 4

Test e implementaciones

En el presente capítulo, se presenta el test de primalidad con curvas elípticas Goldwasser-Killian que se utiliza para determinar si un número de muchos dígitos n es un número primo o no. Dicho test se puede implementar a través de algoritmos en los cuales se pone en marcha y muestra la efectividad del test de primalidad de nuestro estudio. En este caso en particular, lo ejecutaremos en el sistema algebraico computacional magma.

4.1 Test de primalidad con curvas elípticas Goldwasser-Killian

Teorema 4.1. *Sea $n > 1$ y sea E una curva elíptica módulo n. Supongamos que existen distintos números primos $l_1, ..., l_k$ y los puntos finitos $P_i \in E(\mathbb{Z}_n)$ tal que*

1. *$l_i P_i = \infty$ para $1 \leq i \leq k$*

2. *$\prod_{i=1}^{k} l_i > (n^{\frac{1}{4}} + 1)^2$*

Entonces n es primo.

Demostración 4.1. Sea p un factor primo de n. Escribimos $n = p_{n_1}^f$ con $p \nmid n_1$, entonces

$$E(\mathbb{Z}_n) = E(\mathbb{Z}_{p^f}) \oplus E(\mathbb{Z}_{n_1})$$

Como P_i es un punto finito en $E(\mathbb{Z}_n)$ y esto produce un punto finito en $E(\mathbb{Z}_{p^f})$, llamado P_i mód p^f. Podemos reducir aún más y tener el punto finito $P_{i,p} = P_i(\text{mód}p)$ en $E(\mathbb{F}_p)$. Como $l_i P_i = \infty$ mód n, tenemos $l_i P_i = \infty$ módulo cada

factor de n. En particular, $l_i P_{i,p} = \infty$ en $E(\mathbb{F}_p)$, lo que significa que $P_{i,p}$ tiene orden l_i. Se deduce que

$$l_i | \#E(\mathbb{F}_p)$$

para toda i, entonces $\#E(\mathbb{F}_p)$ es divisible por $\prod l_i$. Por lo tanto,

$$(n^{\frac{1}{4}} + 1) < \prod_{i=1}^{k} l_i \leq \#E(\mathbb{F}_p < p + 1 + 2\sqrt{2} = (p^{\frac{1}{2}} + 1)^2$$

entonces $p > \sqrt{n}$. Como todos los factores primos de n son mayores que $\sqrt{n}$, resulta que n es primo.

4.2 Algoritmos

Algoritmo 3: Generar curva $E(\mathbb{F}_p)$.

1. Generar aleatoriamente (A, B) hasta que $(4A^3 + 27B^2, p) = 1$.
2. Calcular $\#E_p(A, B)$ usando el algoritmo de Schoof. Si el número es impar, volver al paso 1. De otra manera, establecer $q = \#E_p(A, B)/2$.
3. Ejecutar el test probabilístico de Miller-Rabin en q para probar $2k$ (donde p tiene k dígitos). Si alguna de las pruebas genera resultados compuestos, volver al paso 1. Si es 2, $3/q$, volver al paso 1.
4. Devuelve $((A, B), q)$

Primero elegimos aleatoriamente A, B tal que $\text{mcd}(4A^3 + 27B^2, p) = 1$ y $\#E_p(A, B) = 2q$ para algún primo q. Calculamos el tamaño de $\#E_p(A, B)$, utilizando el algoritmo de Schoof, y comprobamos que $\#E_p(A, B) = 2q$. La primalidad de q la comprobamos utilizando un algoritmo de prueba de primalidad estándar. Repetimos los pasos hasta que (A, B) pase ambos controles.

Ejemplo 4.2.1. *Sea* $p = 911$*, generamos la curva* $y^2 = x^3 + 679x + 698$*, con su discriminante primo relativo con p. Calculamos* $\#E_p = 958$*, y obtenemos* $q = 479$ *que es primo, como lo requiere el algoritmo.*

Algoritmo 4: Elegir un punto (p,q,(A,B)).

1 Escoger aleatoriamente x de Z_p hasta que $z = x^3 + Ax + B$ sea un residuo cuadrático.

2 Calcular $y = \sqrt{z}$, eligiendo aleatoriamente qué raíz cuadrada de z tomar. Conjunto $L = (x, y)$

3 Calcular qL duplicando repetidamente. Sí $qL \neq 1$, volver al paso 1. De otra manera, devuelve (L).

Ejemplo 4.2.2. *Utilizando la curva generada en el ejemplo anterior con* $p = 911$*, escogemos un* x *hasta que* $z = x^3 + 679x + 698$ *sea un residuo cuadrático. Para* $x = 400$ *tenemos que* $z = 337$*, un residuo cuadrático. Como* $y = \sqrt{z}$ *calculamos* $y = \sqrt{337} = 149$ *por lo que el punto seleccionado es* $L = (400, 149)$*. Finalmente* $479L = \infty$*, pasando todos los controles.*

Algoritmo 5: Paso principal (p)

1 Calcular $((A, B), q)$ utilizando **Generar curva (p)**, y L utilizando **Elegir un punto (p,q,(A,B))**.

2 Devuelve $((A, B), L, q)$

Ejemplo 4.2.3. *Para el paso principal utilizamos los algoritmos anteriores con* $p = 1117$*. Con el* ***algoritmo 2*** *obtenemos la curva* $y^2 = x^3 + 516x + 322$*, luego utilizamos* ***algoritmo 3*** *encontrando el punto* $L = (977, 34)$ *y* $q = 577$*.*

Algoritmo 6: Prueba de primalidad (p)

1 Definir $i = 0$, $p_0 = p$ y el límite inferior=$max(2^{k^{C/lglgk}}, 37)$, donde p tiene k dígitos.

2 Mientras $p_i >$ límite inferior, hacer

$$(A_i, B_i), L_i, p_{i+1} \text{ utilizando } \textbf{Paso principal (p)}$$

y el conjunto $i = i + 1$. Volver al paso 1 si ningún p_i es divisible por 2 o 3.

3 Usando un algoritmo determinístico, verificár si p_i es primo. Si p_i no es primo, ir al paso 1. De otra manera

$$\text{Devuelve } ((A_0, B_0), L_0, p_1), ..., ((A_{i-1}, B_{i-1}), L_{i-1}, p_i)$$

La prueba de primalidad (p) constituye un certificado de primalidad de p que puede ser determinista comprobado en el tiempo O $(|p|^4)$. El verificador probabilistico funciona de la siguiente forma:
$p, ((A_0, B_0), L_0, p_1), ..., ((A_{i-1}, B_{i-1}), L_{i-1}, p_i)$

El Algoritmo 7 verifica que p_i es suficientemente pequeño para ser verificado por el algoritmo de Cohen y Lenstra (1984), y aborta si este no es el caso. Luego verifica que p_i es primo y aborta si no es el caso. Luego, para $j = 1, ..., i-1$, se verifica que
- p_j no es divisble por 2 o 3
-(A_j, B_j) es una curva sobre Z_p
- ${p_{j+1}} > {p_j}^{1/2} + 2{p_j}^{1/4} + 1$
- $\infty_{p_j}, q_j L_j = \infty_{p_j}$

Algoritmo 7: Verificador $(p, ((A_0, B_0), L_0, p_1), ..., ((A_{i-1}, B_{i-1}), L_{i-1}, p_i))$

1 Abortar sí $p_i > max(2^{k^{C/lglgk}}, 37)$ donde p tiene k dígitos. De otra manera, probar la primalida de p_i.

2 Definir $p_0 = p$. Para $j \in [0, i-1]$, verificar que

- p_i no es divisible por 2 o 3.
- $(4{A_j}^3 + 27{B_j}^2, p_j) = 1$
- ${p_{j+1}} > {p_j}^{1/2} + 2{p_j}^{1/4} + 1$
- $L_j \neq \infty_{p_j}, q_j L_j = \infty_{p_j}$

Si no cumple ninguna de estas condiciones, abortar. De otra manera, aceptar p como primo.

El algoritmo completo se basa en repetir el algoritmo de reducción principal hasta que el primo probado sea tan pequeño que permita verificarse un polinomio primo. También existe una condición de aborto, para que se reinicie después de que se hayan realizado suficientes pasos. cuando existe un error en la prueba de primalidad probabilística hace que el algoritmo se atasque al intentar probar un número primo. Para la ejecución de este algoritmo, dejamos que la constante C se defina como una constante positiva de modo que la prueba de primalidad de Cohen-Lenstra [3] tome tiempo O (k) en entradas de tamaño $2^{(k)c/lg/lgk}$ se verifica que existe una constante positiva.

Ejemplo 4.2.4. *Utilizaremos el algoritmo en reiteradas ocasiones para reducir* $p = 1193$ *y saber si es primo. Al repetir el algoritmo deberiamos obtener una sucesión de números primos hasta que* p_i *sea un primo conocido.*
La sucesión resultante es:

p	$x^3 + Ax + B$	q	L
1193	$x^3 + 1175x + 326$	571	(678 , 225)
571	$x^3 + 5x + 558$	281	(515 , 124)
281	$x^3 + 209x + 278$	149	(233 , 259)
149	$x^3 + x + 94$	83	(72 , 136)
83	$x^3 + 37x + 57$	37	(67 , 10)

Como 37 *es primo, todos los números que pertenecen a la sucesión son primos, por lo tanto, probamos la primalidad de 1193.*

Ejemplo 4.2.5. *Para* $p = 1000678854561457$ *tenemos la curva* $y^2 = x^3 + 56344464356629x + 927257163322298$ *y el punto* $L = (867706916191752, 249491136604519)$
La sucesión que obtenemos utilizando esa curva es:

[1000678854561457, 500339414441753, 250169720424259, 125084849171873, 62542423131719, 31271209512563, 15635601124331, 7817802098563, 3908901237503, 1954451619689, 977225924957, 488612862457, 244305949211, 122152641209, 61076454347, 30538294823, 15269124769, 7634526593, 3817290649, 1908647899, 954293201, 477154219, 238581839, 119290487, 59645633, 29824709, 14915393, 7459093, 3729499, 1864483, 931289, 465781, 233201, 116903, 58661, 29437, 14759, 7457, 3769, 1907, 953, 499, 233, 127, 73, 29]

Como 29 *es primo, todos los números que pertenecen a la sucesión son primos, así probamos la primalidad de* 1000678854561457.

Por lo tanto, para saber si grandes números, con cientos o miles de dígitos, son primos, utilizamos sucesivamente el algoritmo para reducirlo hasta llegar a un primo conocido. En general esta versión usa un algoritmo determinista para probar si p_i es primo. Ver en [4].

MAGMA

El desarrollo de investigaciones en las distintas áreas de la matemática se ha visto agilizado gracias a los avances tecnológicos. Para realizar algunos cálculos utilizamos Magma, un sistema de álgebra computacional (CAS). Es un paquete de software grande y bien soportado, diseñado para cálculos en álgebra, teoría de números, geometría algebraica y combinatoria algebraica. Proporciona un entorno matemáticamente riguroso para definir y trabajar con estructuras como grupos, anillos, campos, módulos, álgebras, esquemas, curvas, gráficos, diseños, códigos y muchos otros. Magma también admite una serie de bases de datos diseñadas para ayudar a la investigación computacional en aquellas áreas de las matemáticas que son de naturaleza algebraica.

4.3 Funciones básicas en Teoría de números

- Para obtener la factorización en números primos de un número n dado usamos:

  ```
  > Factorization(123456);
  [<2,6>,<3,1>,<643,1>]
  ```

  Esto significa que $123456 = 2^6 \cdot 3 \cdot 643$

- El resto y el cuociente cuando a es dividido por b.

  ```
  > Quotrem(16,7)
  2 2
  ```

- Calcular el máximo común divisor entre a y b.

  ```
  > GCD(332,676);
  ```

```
4
```

Aritmética Modular

- Para calcular a quién es congruente el número dado.

  ```
  > 12 mod 5
  2
  ```

  O sea $12 \equiv 2$ mód 5

- Para calcular la potencia n^k mód m donde $n, k, m \in \mathbb{Z}$ y $m > 1$.

  ```
  > modex(2,340,341);
  1
  ```

  O sea $2^{340} \equiv 1$ mód 241

- Para calcular el inverso u de n módulo m, esto es $u \cdot n \equiv 1$ mód m donde $1 \leq u < n, k, m \in \mathbb{Z}$ y $mcd(m, n) = 1$.

  ```
  > Modinv(2,341);
  171
  ```

- Otra forma para calcular el inverso de u de n módulo m, esto es $u \cdot n \equiv 1$ mód m dónde $1 \leq u < n, k, m \in \mathbb{Z}$ y $mcd(m, n) = 1$.

  ```
  > InverseMod(2,341);
  171
  ```

- Para calcular el orden, es decir el menor entero $k > 1$ tal que $n^k \equiv 1$mód m.

  ```
  > Modorder(2,341)
  10
  ```

Primalidad

- Para verifcar si un número es primo (probable) escribe true (verdadero) si n es primo y false (falso) si n no es primo.

```
> IsPrime(12);
false
```

```
> IsPrime(17);
true
```

```
> IsPrime(2^32 + 1);
false
```

IsPrime se puede usar como comando para chequear primalidad probabilística; Si el output es true, existe una posibilidad de que el número no sea primo.

- Para chequear si n es un primo probable.

```
> IsProbablePrime(534671892034)
false
```

```
> IsProbablePrime(384583591801)
true
```

- Para calcular el primo más pequeño que es más grande que n.

```
> NextPrime(3)
5
> NextPrime(7)
11
```

Cuerpos finitos

- Crear el cuerpo $\mathbb{F}_q$ con $q = p^n$ donde p es un primo.

```
> FiniteField(11)
Finite field of size 11
```

```
> FiniteField(7^2)
Finite field of size 11^2

> FiniteField(11,2)
Finite field of size 11^2

> GaloisField(7)
7

> GF(7)
Finite field of size 11
```

Iteraciones y condicionales

- Las declaraciones iterativas son similares a las de otros leguajes de programación.

for variable **in do**
declaraciones
end for;

```
> for i:=0 to 5 do 2^(2^i) mod 1000; end for;
2
4
16
256
536
296
```

while Expresión booleana **do**
declaraciones
end while;

```
> y:=24;
> while IsSquare(y^2 - 561) eq false do y := y + 1;end while;
> y
25
```

repeat
declaraciones
until expresión booleana;

```
> y:=24;
> repeat y := y + 1; until IsSquare (y^2 - 561) eq true;
> y;
25
```

if expresión booleana 1
then declaración 1
elif expresión booleana 2
then declaración 1
else declaración 1
end if;

```
> if IsPrime(17), ''Es primo''; else 17, ''es compuesto''; end if;
17 es primo
```

Notar que **elif** proporciona una abreviatura para **else if**.

Definir funciones

- Para definir una función, la estructura básica es la siguiente:

nombre:=function(entrada)
return(salida);
end function;

4.4 Curvas elípticas

- Curva elíptica

```
> F:=GF(23);
> p<x>:=PolynomialRing(F);
```

```
> f:=x^3 + 5 * x + 2;
> E:=EllipticCurve(f);
```

- Orden de la curva E

```
> #E;
21
```

- Puntos de la curva E

```
> Points(E);
```

$(0 : 1 : 0), (0 : 5 : 1), (0 : 18 : 1), (1 : 10 : 1), (1 : 13 : 1), (6 : 8 : 1), (6 : 15 : 1),$
$(7 : 9 : 1), (7 : 14 : 1), (8 : 5 : 1), (8 : 18 : 1), (11 : 10 : 1), (11 : 13 : 1),$
$(15 : 5 : 1), (15 : 18 : 1), (17 : 3 : 1), (17 : 20 : 1), (18 : 6 : 1), (18 : 17 : 1),$
$(20 : 11 : 1), (20 : 12 : 1)$

- Suma de puntos de E

```
> P:=E![1,10];
> Q:=E![11,10];
> P+Q;
(11 : 13 : 1)
```

- Punto de multiplicación

```
> 21*P;
(0 : 1 : 0)
```

- Punto aleatorio de E

```
> Random(E);
(20 : 12 : 1)
```

4.5 Test Goldwasser-Killian

A continuación se presenta la implementación de algunos de los algoritmos utilizados para hacer ejemplos del Test Goldwasser-Killian

```
> GeneraCurva:=function(p);
> repeat
> repeat
> A:=Random(p-1);
> B:=Random(p-1);
> until GCD(4 * A^3 + 27 * B^2, p)eq1;
> E:=EllipticCurve([GF(p)|A,B]);
> until (#E mod 2 eq 0) and IsProbablePrime(#E div 2) eq true;
> return Integers()!A, Integers()!B, E, #E div 2;
> end function;

> SeleccionarPunto:=function(p,q,A,B)
> E:=EllipticCurve([GF(p)|A,B]);
> repeat
> repeat
> x:=Random(0,p-1);
> yy:=(Modexp(x, 3, p) + A * x + B) mod p;
> until JacobiSymbol(yy,p) ne -1;
> y:=Modsqrt(yy,p);
> L:=E![x,y];
> until q*L eq E!0;
> return Integers()!L[1],Integers()!L[2]];
> end function;

> PasoPrincipal:=function(p)
> A,B,E,q:=GeneraCurva(p);
> L:=SeleccionarPunto(p,q,A,B);
> return A,B,q,L;
> end function;
```

Bibliografía

[1] Basso, I. Riquelme, E. (2017). *Apuntes básicos de criptografía.*

[2] Belingueres, G. (2001). *Introducción a los criptosistemas de curva elíptica.*

[3] Cannon, J. Playoust, C. (1996). *First Steps in Magma.*

[4] Cohen, H. Lenstra, H. W., Jr. (1984). *Primality testing and Jacobi sums. Math.* Comp. 42(165): 197-330.

[5] Condori, S. (2016). *Estudio de los tests de primalida.*

[6] Fraleigh, J. (1988). *A first course in abstract algebra.* Addison-Wesley.

[7] Goldwasser, S. Killian, J. (1999). *Primality testing using elliptic curves.* Journal of the ACM 46(4), 450-472.

[8] Gracián, E. (2010). *Los números primos. Un largo camino al infinito.* El mundo es matemático. Navarra, España. RBA Coleccionables.

[9] Hankerson, D. Menezes, A. Scott, V. (2003). *Guide to elliptic curve cryptography.* Springer.

[10] Judson, Thomas W. (1994). *Abstract Algebra: Theory and Applications*

[11] Schoof, R. (2008). *Four primality testing algorithms.* Algorithmic Number Theory 44.

[12] Washington, L. (2008). *Elliptic Curves: Number Theory and Criptography, Second Edition.* Discrete mathematics and its applications.