UNA INTRODUCCIÓN A LA CRIPTOGRAFÍA Y LA TEORÍA DE CÓDIGOS

JESÚS JIMÉNEZ REYES

Índice

1. Introducción

Estas notas tienen el propósito de presentar al lector el uso de las matemáticas en el diseño de códigos correctores de errores y cifrados. Los códigos y los cifrados juegan un papel fundamental en la transmisión de datos digitales en medios de comunicación. Por ejemplo, la televisión, la telefonía celular, los discos compactos, comercio electrónico, etcetera.

2. Preliminares

2.1. Propiedades elementales de los números enteros. El conjunto de los números enteros, denotado por el símbolo $\mathbb{Z}$, es el conjunto

$$\mathbb{Z} = \{..., -4, -3, -2, -1, 0, 1, 2, 3, 4, ...\}.$$

Existen dos operaciones binarias definidas sobre el conjunto $\mathbb{Z}$, la suma (denotada por $a+b$) y la multiplicación (denotada por ab). Estas dos operaciones satisfacen las siguientes propiedades.

1. Propiedades de la suma:

Date: Junio–Julio 2026.

a) Conmutatividad. Para todo par de números enteros a y b,

$$a+b=b+a$$

b) Asociatividad. Para toda terna de números enteros a, b, y c,

$$(a+b)+c=a+(b+c)$$

c) Elemento neutro aditivo. Existe un número entero, 0, llamado cero, tal que para todo número entero a,

$$a+0=a$$

d) Elemento inverso aditivo. Para todo número entero a, existe un número entero b, tal que

$$a+b=0$$

2. Propiedades de la multiplicación:
   a) Conmutatividad. Para todo par de números enteros a y b,

$$ab=ba$$

   b) Asociatividad. Para toda terna de números enteros a, b, y c,

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

   c) Elemento neutro multiplicativo. Existe un número entero, 1, llamado uno, tal que para todo número entero a,

$$a1=a$$

   d) Distributividad. Para toda terna de enteros a, b, y c

$$(a+b)c=ac+bc$$

3. Ley de cancelación. Si a, b, y $c\neq 0$ son números enteros y $ca=cb$ entonces $a=b$. La ley de cancelación ies equivalente a: si $ab=0$ entonces $a=0$ ó $b=0$.

Definición 1. *Sea R un conjunto que contiene al menos dos elementos 0 y 1, $0\neq 1$ y dotado de dos operaciones: la suma $a+b$ y la multiplicación o producto ab tal que $a+b$ y ab son elementos de R y que la suma y producto satisfacen las propiedades $1a)-1b)$ y $2a)-2b)$. Entonces R es llamado un* ***anillo conmutativo****. Si además la ley de cancelación es válida en R entonces R es llamado un* ***dominio entero****.*

2.2. Orden.

Definición 2. *El conjunto de enteros positivos es el conjunto*

$$\mathbb{Z}^+=\{1,2,3,4,...\}.$$

Las siguientes propiedades de los números enteros positivos seran tomadas como axiomas.

Axioma 3. *La suma de dos números enteros positivos es un número positivo.*

Axioma 4. *El producto de dos números enteros positivos es un número positivo.*

Axioma 5. *Ley de la tricotomía. Dado un número entero a, una y sólo una de las siguientes afirmaciones es cierta: a es positivo, $a=0$, ó $-a$ es positivo.*

Teorema 6. *Si a es un número entero distinto de cero entonces a^2 es un número entero positivo.*

Demostración. Si a es un número entero positivo entonces $a^2=aa$ es positivo por el axioma 4. Si $-a$ es positivo entonces $(-a)(-a)$ es positivo por el axioma 4. Demuestre que $(-a)(-a)=a^2$ para terminar la demostración de el teorema. □

Definición 7. ***Orden sobre los números enteros.*** *Si a y b son números enteros definimos $a<b$ (lease a menor que b) si $b-a$ es un número entero positivo. Observese que $0<b$ si y sólo si $b=b-0$ es un número entero positivo.*

Teorema 8. *Sean a, b y c números enteros.* (1) *Si $a<b$ y $b<c$ entonces $a<c$.* (2) *Si $a<b$ entonces $a+c<b+c$.* (3) *Si $a<b$ y $0<c$ entonces $ac<bc$.* (4) *Si $a<b$ y $c<0$ entonces $bc<ac$.*

Demostración. Ejercicio. □

Definición 9. *Sea a un número entero. Definimos el* ***valor absoluto*** *de a, denotado $|a|$, de la siguiente manera:*

$$|a| = \begin{cases} a & si\ a > 0 \\ 0 & si\ a = 0 \\ -a & si\ a < 0 \end{cases}$$

2.3. Principio del buen orden.

Definición 10. *Sea $<$ el orden sobre los números enteros definido anteriormente. Sea S un subconjunto no vacío de los números enteros. El orden $<$ es un buen orden sobre S si cada subconjunto no vacío de S contiene un elemento mínimo con respecto a $<$.*

Axioma 11. ***Principio del buen orden.*** *El orden $<$ es un buen orden sobre los enteros positivos. Es decir, dado un subconjunto no vacío W de los números enteros positivos existe un elemento w_{min} en W tal que $w_{min} \leq w$ para todo w en W.*

Teorema 12. *No existe un número entero n tal que $0 < n < 1$.*

Demostración. Supongamos que existe un número entero n con la propiedad $0 < n < 1$. Sea S el subconjunto de los enteros positivos definido por la siquiente propiedad: s esta en S si y sólo si $0 < s < 1$. Por hipótesis S es no vacío. Por el principio del buen orden S tiene un elemento mínimo. Llamemos m a este elemento. Así que $0 < m < 1$. Multiplicando la última desigualdad por m obtenemos $0 < m^2 < m$. Así que $0 < m^2 < m$ y $0 < m^2 < 1$. Estas ultima desigualdad implica que m^2 esta en S. Sin embargo $m^2 < m$, lo cual es una contradicción. Por lo tanto S es vacío. □

Teorema 13. ***Primer principio de inducción finita.*** *Sea S un subconjunto no vacío de los números enteros positivos. Supongamos que 1 es elemento de S y que cada vez que n está en S, $n+1$ está en S entonces S es el conjunto de los números enteros positivos.*

Demostración. Sea S' el subconjunto de números enteros positivos que no están en S. Es suficiente demostrar que S' es vacío. Supongamos que S' es no vacío. Por el principio del buen orden S' tiene un elemento mínimo s'. $s' \neq 1$ ya que 1 está en S. Ademas, $s' > 1$ por el teorema 12. Así que $s' - 1$ es un número entero positivo. Como $-1 < 0$ (demuéstrese esto) se sigue que $s' - 1 < s'$. Por lo tanto $s' - 1$ no está en S'. Esto es $s' - 1$ está en S. Por hipótesis, $(s' - 1) + 1$ esta en S. Esto implica que s' está en S, lo cual es una contradicción pues s' esta en S' no en S. Se concluye que S' es vacío y por lo tanto S es el conjunto de los números enteros positivos □

Teorema 14. ***Segundo principio de inducción finita.*** *Sea S un subconjunto no vacío de los números enteros positivos. Supongamos que cada vez que $1, 2, ..., n$ está en S, $n+1$ está en S entonces S es el conjunto de los números enteros positivos.*

Demostración. Ejercicio □

2.4. Divisibilidad. La ecuación $ax = b$ puede no tener solución en los números enteros. Por ejemplo, no existe un número entero x tal que $3x = 5$. En otras ocaciones como en el caso $3x = 6$ la ecuación tiene solución en los números enteros. En esta situación decimos que 6 es un múltiplo de 3 ó que 3 divide a 6 ó que 3 es un factor ó divisor de 6.

Definición 15. *Sean a y b números enteros. Decimos que a divide a b si existe un número entero q tal que $b = aq$. Usaremos la notación $a \mid b$ para indicar que a divide a b y $a \nmid b$ para indicar que a no divide a b.*

Definición 16. *Un número entero a es una unidad de los número enteros si $a \mid 1$.*

Teorema 17. *Las unidades de los números enteros son 1 y -1.*

Demostración. Supongamos que $a \mid 1$. Entonces existe q tal que $aq = 1$. Hay dos casos $a > 0$ y $q > 0$ ó $-a > 0$ y $-q > 0$ (porque?). Supongamos que $a > 0$ y $q > 0$. Recuérdese que como $a > 0$, $a \geq 1$. Similarmente $q \geq 1$. Si $a > 1$, entonces $aq > q \geq 1$. Esto es una contradción puesto que $aq = 1$. De manera similar no se puede tener $q > 1$. Por lo tanto $a = 1$ y $q = 1$. El caso $-a > 0$ y $-q > 0$ se deja como ejercicio. □

Corolario 18. *Si $a \mid b$ y $b \mid a$ entonces $a = b$ ó $a = -b$.*

Demostración. Ejercicio □

Proposition 19. *Si a, b, y c son números enteros tal que $a \mid b$ y $b \mid c$, entonces $a \mid c$.*

Demostración. Ejercicio □

Proposition 20. *Si a, b, c, r, y s son números enteros tal que $c \mid a$ y $c \mid b$ entonces $c \mid (ra + sb)$.*

Demostración. Ejercicio □

Definición 21. *Un número entero p es primo si $p \neq 0$, $p \neq 1$, $p \neq -1$ y los únicos divisores de p son 1, -1, p y $-p$.*

Los primeros cinco números primos son

$$2, 3, 5, 7, 11.$$

2.5. Algoritmo Euclideano y máximo común divisor. El siguiente teorema establece un hecho fundamental acerca de la división de números enteros.

Teorema 22. ***El algoritmo de la división.*** *Si a y b son números enteros con $b > 0$, entonces existen números enteros q y r, únicos, tal que $a = bq + r$ con $0 \leq r < b$.*

Demostración. Consideremos el conjunto

$$S = \{a - bq \mid q \text{ es un número entero no negativo}\}$$

Si 0 es elemento de S entonces $a - bq = 0$ y se sigue que $a = bq + 0$. Supongamos que 0 no está en S. Sea P el subconjunto de S tal que $a - bq$ es un número entero positivo. Afirmamos que P es no vacío. Veamos esto. Por hipótesis $b \geq 1$. Podemos suponer que $b > 1$ porque si $b = 1$ la afirmación del teorema es clara. Multiplicando la desigualdad $b > 1$ por $-|a|$ obtenemos $-|a|\, b < -|a|$ y como $-|a| \leq a$ se sigue que $-|a|\, b < -|a| \leq a$ así que $a - (-|a|\, b) > 0$. Por lo tanto $a - (-|a|\, b)$ está en P.

Por el principio del buen orden P tiene un elemento mínimo, digamos r. Esto es $a - bq = r$ ó $a = bq + r$. Por construcción $r > 0$. Si $r \geq b$ entonces $r > r - b = r' \geq 0$ y se tiene que

$$a = bq + r = bq + b + r - b = b(q + 1) + r'$$

por lo tanto $a - b(q + 1) = r' \geq 0$. Si $r' = 0$ entonces 0 esta en S, lo cual contradice el hecho que 0 no esta en S. Si $r' > 0$ entonces r' esta en P y $r' < r$, lo cual contradice el hecho que r es el elemento mínimo de P.

Se deja como ejercicio demostrar que q y r son únicos. □

Lema 23. *Sea d un número entero positivo. Sea*

$$\mathbb{Z}d = \{nd \mid n \text{ un número entero}\}.$$

Si x y y estan en $\mathbb{Z}d$ y m es un número entero, entonces $x + y$, $x - y$, y mx estan en $\mathbb{Z}d$.

Demostración. Por hipótesis $x = n_1 d$ y $y = n_2 d$. Se sigue que $x + y = n_1 d + n_2 d = (n_1 + n_2)d$, $x - y = n_1 d - n_2 d = (n_1 - n_2)d$ y $mx = m(n_1 d) = (mn_1)d$. Estas igualdades demuestran el lema. □

Teorema 24. *Sea I un subconjunto no vacío de los números enteros que es cerrado bajo sumas y restas entonces $I = \mathbb{Z}d$ para algún número entero positivo d ó $I = \{0\}$.*

Demostración. Supongamos que $I \neq \{0\}$. Sea $a \neq 0$ un elemento de I. Como I es cerrado bajo restas $a - a = 0$ esta en I y por lo tanto $0 - a = -a$ esta tambien en I. Se sigue que I contiene números enteros positivos. Sea I^+ el subonjunto de I formado de los elementos positivos de I. Hemos visto que I^+ es no vacío. El principio del buen orden implica que existe d, d elemento mínimo de I^+. El siguiente ejercicio requiere que el lector demuestre que d satisface la afirmación de el teorema. □

Ejercicio 25. *Demuestre que $I = \mathbb{Z}d$.*

Definición 26. *Sean a y b números enteros. Un número entero d es un máximo común divisor de a y b si d divide a a , d divide a b y cualquier otro divisor de a y b divide a d. Denotaremos el máximo común divisor positivo de a y b (si existe) por* $\operatorname{mcd}(a, b)$.

Teorema 27. *Sean $a \neq 0$ y $b \neq 0$ dos números enteros. El máximo común divisor,* $\mathrm{mcd}(a, b)$*, existe y es una combinación lineal de a y b con coeficientes enteros. Esto es,*

$$\mathrm{mcd}(a, b) = ra + sb,$$

para algunos números enteros r y s.

Demostración. Sea L el subconjunto de los números enteros

$$L = \{ra + sb \mid r, s \text{ son números enteros}\}.$$

Es fácil ver que L es cerrado bajo sumas y restas. Por el teorema 24, $L = \mathbb{Z}d$ para algún número entero positivo $d = ra + sb$. Se sigue de la proposición 20 que cualquier divisor de a y b es un divisor de d. Por otro lado como $a = 1a + 0b$ y $b = 0a + 1b$, se sigue que d divide a a y a b. Así que d es el maximo común divisor positivo de a y b. □

Lema 28. *Sean a y b números enteros y $a = bq + r$ entonces*

$$\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r).$$

Demostración. Como $r = a - bq$, la proposición 20 implica que $\mathrm{mcd}(a, b)$ divide a r. Así que $\mathrm{mcd}(a, b)$ divide a $\mathrm{mcd}(b, r)$. Por otro lado, la proposición 20 implica $\mathrm{mcd}(b, r)$ divide a $a = bq + r$. Así que $\mathrm{mcd}(b, r)$ divide a $\mathrm{mcd}(a, b)$. Se sigue de el corolario 18 que $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r)$ ó $\mathrm{mcd}(a, b) = -\mathrm{mcd}(b, r)$. Como $\mathrm{mcd}(a, b)$ y $\mathrm{mcd}(b, r)$ son positiovos, $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r)$ es la única posibilidad. □

Definición 29. *Dos números enteros a y b son* ***primos relativos*** *si y sólo si* $\mathrm{mcd}(a, b) = 1$.

Lema 30. *Sea p un número primo. Entonces* $\mathrm{mcd}(p, a) = 1$ *ó* $\mathrm{mcd}(p, a) = p$.

Demostración. Sea $d = \mathrm{mcd}(p, a)$. Como d divide a p tenemos que $d = 1$, -1, p, ó $-p$. Como d es positivo, $d = 1$ ó $d = p$. □

Este lema dice que si p es un número primo entonces dado un entero a, p divide a a ó p y a son primos relativos.

Lema 31. *Si p es número primo y $p \mid ab$ entonces $p \mid a$ ó $p \mid b$.*

Demostración. Por el lema anterior $\mathrm{mcd}(p, a) = 1$ ó $\mathrm{mcd}(p, a) = p$. Si $\mathrm{mcd}(p, a) = p$ entonces p divide a a. Por otro lado si $\mathrm{mcd}(p, a) = 1$ entonces existen enteros r y s tal que $ra + sp = 1$. Se sigue que $(ra + sp)b = 1b = b$. Lo cual dice que $rab + spb = b$. Se sigue de la proposición 20 que p divide a $rab + spb$. Esto es, p divide a b. □

Lema 32. *Si* $\mathrm{mcd}(b, a) = 1$ *y $b \mid ac$ entonces $b \mid c$.*

Demostración. Ejercicio □

Lema 33. *Si* $\mathrm{mcd}(a, b) = 1$*, $a \mid m$ y $b \mid m$ entonces $ab \mid m$.*

Demostración. Ejercicio □

2.6. Teorema fundamental de la aritmética. El teorema fundamental de la aritmética establece que todo número entero se puede obtener usando la multiplición de números primos positivos y unidades de los números enteros. He aquí el enunciado preciso de el teorema.

Teorema 34. ***Teorema fundamental de la aritmética.*** *Todo número entero n se puede representar de manera única en la forma*

$$n = +1(p_1 \cdots p_r) \text{ ó } -1(p_1 \cdots p_r)$$

con $p_1, ..., p_r$ números primos positivos.

Demostración. Sin pérdida de generalidad podemos suponer que n es positivo. Si n es primo ó $n = 1$ no hay nada que demostrar. Por lo tanto podemos suponer que n tiene un divisor $d > 1$, Esto es $n = md$. Así que usando el segundo principio de inducción, teorema 14, se tiene que

$$m = (p_1 \cdots p_r) \text{ y } d = (q_1 \cdots q_s)$$

de lo cual se sigue que

$$n = (p_1 \cdots p_r)(q_1 \cdots q_s) = p_1 \cdots p_r q_1 \cdots q_s$$

Esto prueba la existencia de la representacion de n como producto de números primos. Para probar la unicidad, supongamos que n tiene dos representaciones

$$n = p_1 \cdots p_k \text{ y } n = \overline{p}_1 \cdots \overline{p}_l$$

Podemos suponer que $k \leq l$. Como p_1 divide a n se tiene que p_1 divide a $\overline{p}_1 \cdots \overline{p}_l$. Por lo tanto, el lema 31 implica que p_1 divide a $\overline{p}_j$ para alguna $j = 1, 2, ..., l$. Reacomodando los índices podemos suponer que $j = 1$. Se sigue que $p_1 p_2 \cdots p_k = p_1 \overline{p}_2 \cdots \overline{p}_l$ y por la ley de cancelación obtenemos que $p_2 \cdots p_k = \overline{p}_2 \cdots \overline{p}_l$. Repitiendo este proceso k veces obtenemos $1 = \overline{p}_{k+1} \cdots \overline{p}_l$. Esta última igualdad implica que $\overline{p}_{k+1}, ..., \overline{p}_l$ son unidades de los número enteros. Concluimos que la representación es única. □

2.7. Congruencias. Es bien sabido que la manera de contar las horas usando un reloj de manecillas es identificando horas cuya diferencia es un multiplo de 12. Por ejemplo las 19 horas se identifica con las 7 horas. En el lenguage matemático decimos que 19 es congruente con 7 módulo 12 y escribimos $19 \equiv 7$ mód 12. Con esto en mente, hacemos la siguiente definición.

Definición 35. *Sea $m > 1$ un número entero. Definimos $a \equiv b$ mód m si y sólo si $m \mid (a-b)$. Si $a \equiv b$ mód m, diremos que a es congruente con b módulo m. Es fácil ver que $a \equiv b$ mód m si y sólo si $a - b$ es un múltiplo de m, si y sólo si $a = b + mq$.*

Teorema 36. *Supongamos que $a = mq_1 + r_1$ y $b = mq_2 + r_2$ con $0 \leq r_1 < m$ y $0 \leq r_2 < m$. Entonces $a \equiv b$ mód m si y sólo si $r_1 = r_2$. Esto es, a es congruente con b módulo m si y sólo si a y b tienen el mismo residuo al ser divididos por m.*

Demostración. Por definición $a \equiv b$ mód m si y sólo si $m \mid (a - b)$. Se sigue que $a \equiv b$ mód m si y sólo si $m \mid ((mq_1 + r_1) - (mq_2 + r_2)) = (m(q_1 - q_2) + (r_1 - r_2))$, si y sólo si $m \mid (r_1 - r_2)$, si sólo si $r_1 - r_2 = 0$ ya que $|r_1 - r_2| < m$. Así que $r_1 = r_2$. □

Lema 37. *La relación $a \equiv b$ mód m satisface las propiedades siguientes:*

1. Reflexibilidad: $a \equiv a$ mód m.
2. Simetría: si $a \equiv b$ mód m entonces $b \equiv a$ mód m.
3. Transitividad: si $a \equiv b$ mód m y $b \equiv c$ mód m entonces $a \equiv c$ mód m.

Demostración. Ejercicio □

Teorema 38. *Si $a \equiv b$ mód m, entonces para todo número entero c,*

1. $-a \equiv -b$ mód m
2. $a + c \equiv b + c$ mód m
3. $ac \equiv bc$ mód m

Demostración. Demostraremos 1. Sabemos que $a \equiv b$ mód m si y sólo si $m \mid (a-b)$, esto es si y sólo si $m \mid (b-a)$ si y sólo si $-a \equiv -b$ mód m.

Dejaremos 2. y 3. como ejercicios. □

Teorema 39. ***Ley de cancelación.*** *Para todo número entero c tal que*

$$\text{mcd}(m, c) = 1, \ ac \equiv bc \text{ mód } m$$

implica que $a \equiv b$ mód m.

Demostración. Supongamos que $ac \equiv bc$ mód m entonces

$$m \mid (ac - bc) = (a - b)c.$$

Se sigue de el lema 32 que $m \mid (a - b)$. Esto implica que

$$a \equiv b \text{ mód } m.$$

□

Teorema 40. *Si a y m son primos relativos, entonces para todo número entero b existe un número entero x tal que $ax \equiv b$ mód m. Además, si x_1 y x_2 son soluciónes de la congruencia $ax \equiv b$ mód m entonces $x_1 \equiv x_2$ mód m.*

Demostración. Como a y m son primos relativos, existen números enteros r y s tal que $ra + sm = 1$. Por lo tanto $rab + smb = 1b = b$. Sea $x = rb$. Cómo $a(rb) - b = m(sb)$ se sigue que $ax \equiv b$ mód m. Por otro lado si $ax_1 \equiv b$ mód m y $ax_2 \equiv b$ mód m entonces $ax_1 \equiv b$ mód m y $b \equiv ax_2$ mód m por la propiedad de simetría. Por lo tanto, se sigue de la transitividad que $ax_1 \equiv ax_2$ mód m. Concluimos usando la ley de cancelación para congruencias, teorema 39, que $x_1 \equiv x_2$ mód m. □

Corolario 41. *Si p es un número primo y $a \not\equiv 0$ mód p, entonces la congruencia $ax \equiv b$ mód p tiene una solución única.*

Demostración. Ejercicio □

Teorema 42. *Si m_1 y m_2 son primos relativos, entonces las congruencias*

$$x \equiv b_1 \text{ mód } m_1 \text{ y } x \equiv b_2 \text{ mód } m_2$$

tienen una solución común. Cualesquiera dos soluciones son congruentes módulo m_1m_2.

Demostración. Observemos que para todo número entero z, $x = b_1 + zm_1$ es solució de la congruencia $x \equiv b_1$ mód m_1. Entonces, x satisface la segunda congruencia si y sólo si $b_1 + zm_1 \equiv b_2$ mód m_2 o lo que es lo mismo si y sólo si $m_1z \equiv b_2 - b_1$ mód m_2 como m_1 y m_2 son primos relativos. El teorema 40 garantiza que existe un número entero z que satisface la congruencia

$$m_1z \equiv b_2 - b_1 \text{ mód } m_2.$$

Además, si x_1 y x_2 son soluciónes de las congruencias $x \equiv b_1$ mód m_1 y $x \equiv b_2$ mód m_2 entonces $m_1 \mid (x_1 - b_1)$ y $m_1 \mid (x_2 - b_1)$ así que $m_1 \mid ((x_1 - b_1) - (x_2 - b_1)) = x_1 - x_2$. Esto es, m_1 divide a $x_1 - x_2$. Similarmente podemos mostrar que m_2 divide a $x_1 - x_2$. Como m_1 y m_2 son primos relativos, el lema 33 implica que m_1m_2 divide a $x_1 - x_2$. Es decir $x_1 \equiv x_2$ mód m_1m_2. □

El siguiente teorema generaliza al teorema anterior.

Teorema 43 (Teorema chino del residuo)**.** *Si m_1, m_2, ... , m_k son primos relativos por pares. Entonces las congruencias*

$$\begin{aligned} x &\equiv b_1 \text{ mód } m_1 \\ x &\equiv b_2 \text{ mód } m_2 \\ &\vdots \\ x &\equiv b_k \text{ mód } m_k \end{aligned}$$

tienen una solución simultánea. Además, cualesquiera dos soluciones son congruentes módulo el producto $M = m_1m_2 \cdots m_k$.

Demostración. Demostraremos la existencia de la solución. La segunda parte se deja como ejercicio. Definamos $M_i = M/m_i$ para $i = 1, 2, \ldots, k$. Por hipótesis y construcción, M_i y m_i son primos relativos, se sigue de el teorema 40 que la congruencia

$$M_iN_i \equiv 1 \text{ mód } m_i$$

tiene una solución N_i para $i = 1, 2, \ldots, k$. Sea

$$x = b_1M_1N_1 + b_2M_2N_2 + \cdots + b_iM_iN_i + \cdots + b_kM_kN_k.$$

Se sigue que

$$x - b_iM_iN_i = b_1M_1N_1 + \cdots + b_{i-1}M_{i-1}N_{i-1} + b_{i+1}M_{i+1}N_{i+1} + \cdots + b_kM_kN_k.$$

Como cada sumando en el lado derecho de la última igualdad es divisible por m_i la suma es divisible por m_i. Por lo tanto $x - b_iM_iN_i$ es divisible por m_i. Esto es

$$x \equiv b_iM_iN_i \text{ mód } m_i.$$

Como $M_iN_i \equiv 1$ mód m_i, se tiene que

$$b_iM_iN_i \equiv b_i \text{ mód } m_i.$$

Por la propiedad transitiva de congurencias se concluye que

$$x \equiv b_i \text{ mód } m_i.$$

Por lo tanto x es una solución simultánea de las congruencias dadas. □

Sea n un número entero y $m > 1$. Por el algoritmo de la división $n = mq + r$ con $0 \leq r < m$. Se sigue que $n - r$ es divisible por m. Esto es, $n \equiv r \bmod m$. Como r es el único número entero con la propiedad $0 \leq r < m$, se sigue que para todo número entero n existe un único número entero no negativo r, menor que m, tal que n es congruente con r módulo m.

Definición 44. *Llamaremos a un conjunto*

$$\{r_1, r_2, ..., r_m\}$$

un sistema completo de representantes de los residuos módulo m si para todo número entero n, $n \equiv r_i$ mód m para un único r_i. Hemos observado que el conjunto

$$\{0, 1, 2, 3, ..., m-2, m-1\}$$

es un sistema completo de representantes de los residuos módulo m.

Teorema 45 (Pequeño teorema de Fermat)**.** *Sea p un número primo. Si a es número entero entonces*

$$a^p \equiv a \text{ mód } p.$$

Además, si a y p son primos relativos

$$a^{p-1} \equiv 1 \text{ mód } p.$$

Demostración. Supongamos primero que a y p son primos relativos. Consideremos los números enteros

$$a, 2a, 3a, ..., (p-2)a, (p-1)a.$$

Ninguno de estos números enteros es divisible por p. Además, si $1 \leq i, j \leq p-1$ entonces p tampoco divide a $ia - ja$, es decir ia y ja no tienen el mismo residuo al ser divididos por p. Esto es, el conjunto

$$\{a, 2a, 3a, ..., (p-2)a, (p-1)a\}$$

es un sistema completo de representantes de los residuos módulo m. Por lo tanto,

$$(a)(2a)\cdots((p-2)a)((p-1)a) \equiv (1)(2)\cdots(p-2)(p-1) \text{ mód } p.$$

Así que,

$$a^{(p-1)}(2)\cdots(p-2)(p-1) \equiv (2)\cdots(p-2)(p-1) \text{ mód } p.$$

Como, $i \not\equiv 0$ mód p para $i = 2, 3, ..., (p-1)$ podemos aplicar la ley de cancelación, teorema 39, $p-2$ veces y concluir que

$$a^{(p-1)} \equiv 1 \text{ mód } p.$$

La segunda parte de el teorema se deja como ejercicio. □

2.8. El anillo $\mathbb{Z}_n$. Sea $n > 1$ un número entero y denotemos por $\mathbb{Z}_n$ el subconjunto de números enteros definido como sigue:

$$\mathbb{Z}_n = \{0, 1, 2, 3, ..., n-2, n-1\}.$$

Dados a y b en $\mathbb{Z}_n$ definimos $a \oplus b$ mód $n = g$ donde g es el único elemento de $\mathbb{Z}_n$ tal que

$$a + b \equiv g \text{ mód } n.$$

Similarmente, definimos $a \odot b$ mód $n = h$ donde h es el único elemento de $\mathbb{Z}_n$ tal que

$$ab \equiv h \text{ mód } n.$$

Por definición $\mathbb{Z}_n$ es cerrado con respecto a las operaciones $\oplus$ y $\odot$.

Teorema 46. *El conjunto $\mathbb{Z}_n$ dotado de las operaciones $\oplus$ y $\odot$ es un anillo conmutativo.*

Demostración. Se sigue de el teorema 38 que $\oplus$ y $\odot$ estan bien definidades y son cerradas. El residuo 0 es el elemento neutro aditivo y el residuo 1 es el elemento neutro multiplicativo. El elemento inverso aditivo de r es $n - r$. Demostremos que $a \oplus b \bmod n = b \oplus a \bmod n$, esto es, que la suma es conmutativa. Por definición $a \oplus b \bmod n = g$, donde g es el único elemento de $\mathbb{Z}_n$ tal que $a + b \equiv g \bmod n$ y como $a + b = b + a$ en los números enteros, se sigue que la suma es conmutativa. La demostración de las otras propiedades se hace de manera similar ya que las propiedades son ciertas para los números enteros. □

Por abuso de notación es criberemos $a + b$ y ab en lugar de

$$a \oplus b \bmod n \text{ y } a \odot b \bmod n$$

para a y b elementos de $\mathbb{Z}_n$.

Teorema 47. *El anillo $\mathbb{Z}_p$ es un dominio entero si y sólo si p es un número primo.*

Demostración.

$\mathbb{Z}_p$ es un dominio entero	si y sólo si
$ab = 0$ en $\mathbb{Z}_p$ implica $a = 0$ ó $b = 0$	si y sólo si
$p \mid ab$ implica $p \mid a$ ó $p \mid b$	

Si p es un número primo entonces se sigue de el lema 31 que si $p \mid ab$ entonces $p \mid a$ ó $p \mid b$.

Por otro lado, si p no es primo entonces $p = ab$ con $1 < a < p$ y $1 < b < p$, esto es $a \neq 0$ y $b \neq 0$ en $\mathbb{Z}_p$, pero como $ab = p$, $ab = 0$ en $\mathbb{Z}_p$. Por lo tanto, $\mathbb{Z}_p$ no es un dominio entero. Esto es una contradicción, así que p tiene que ser un número primo. □

Definición 48. *Sea $\mathbb{F}$ un dominio entero. Si para todo elemento a en $\mathbb{F}$, $a \neq 0$ existe b en $\mathbb{F}$ tal que $ab = 1$ entonces decimos que $\mathbb{F}$ es un campo. Nótese que por la ley de cancelación, si b existe, b es único.*

Teorema 49. *El dominio entero $\mathbb{Z}_p$ es un campo.*

Demostración. Esto se sigue inmediatamente de el corolario 41. □

3. Criptografía y cifrados

Un **cifrado** es un algoritmo que se usa para transformar un mensaje en otro mensaje, mensaje-cifrado, de tal manera que sea muy difícil saber el significado de el mensaje original teniendo sólo conocimiento de el mensaje-cifrado. La criptología se divide en dos ramas: **criptografía** y **criptoanálisis**. La **criptografía** es la disciplina en la que uno se dedica a la construcción de cifrados; el **criptoanálisis** es la rama en la que uno se dedica a descubrir el significado o contenido de un mensaje-cifrado sin tener conocimiento de el cifrado usado. **Cifrar** es el proceso de transformar un mensaje en un mensaje-cifrado. **Descifrar** es el proceso de descubrir el significado de un mensaje-cifrado. Por supuesto que para quien ha creado el mensaje-cifrado descifrar el mensaje-cifrado tiene que ser fácil, de otra manera la utilidad del los cifrados sería limitada. Empezaremos por presentar un cifrado atribuido a *Julio César*. En todos los cifrados que construiremos el primer paso será transformar el mensaje escrito en elementos de un conjunto con estructura algebraica. La manera mas sencilla es identificar las letras de nuestro alfabeto con elementos de algún conjunto de éste tipo. Por ejemplo, podemos identificar las letras de el alfabeto con elementos de $\mathbb{Z}_{26}$.

Ejemplo 50. ***Cifrado de Julio César.*** *Identifiquemos las letras de el alfabeto $\{A,\ B,\ C, ..., Z\}$ con los elementos de $\mathbb{Z}_{26}$. Esto es, remplacemos cada ocurrencia de la letra a en nuestro texto por el elemento 0, cada ocurrencia la letra b por 1, cada ocurrencia la letra c por 2, y así sucesivamente hasta llegar a la z la cual será remplazada por el elemento 25. Por ejemplo, el texto:*

$$\textsf{mensaje} : L, A, V, I, D, A, N, O, V, A, L, E, N, A, D, A$$

será transformado en:

$$\textit{mensaje numérico} : 11, 0, 21, 8, 3, 0, 13, 14, 21, 0, 11, 4, 13, 0, 3, 0$$

Después de esto sumemos 17 módulo 26 a cada término de el mensaje númerico para obtener el mensaje numérico:

$$\textit{mensaje numérico mas } 17 : 2, 17, 12, 25, 20, 17, 4, 5, 12, 17, 2, 21, 4, 17, 20, 17$$

Luego convertimos éste mensaje numérico en el mensaje:

$$\textit{mensaje cifrado} : C, R, M, Z, U, R, E, F, M, R, C, V, E, R, U, R$$

Para descifrar el mensaje es suficiente convertir el mensaje cifrado a el mensaje numérico y sumar 9 *módulo* 26 *a cada término de el mensaje numérico. Despues remplazamos los términos en el "mensaje numérico más* 9" *por letras de el alfabeto, así obtenemos:*

$$\textit{mensaje numérico} : 2, 17, 12, 25, 20, 17, 4, 5, 12, 17, 2, 21, 4, 17, 20, 17$$

$$\textit{mensaje numérico más } 9 : 11, 0, 21, 8, 3, 0, 13, 14, 21, 0, 11, 4, 13, 0, 3, 0$$

$$\textit{mensaje descifrado} : L, A, V, I, D, A, N, O, V, A, L, E, N, A, D, A$$

En éste ejemplo el número 17 recibe el nombre de **clave para cifrar** y al número 9 se le llama **clave para descifrar**. Tambien es claro en este ejemplo, que con un poco de esfuerzo uno podría ser capáz de descifrar el mensaje sin tener conocimiento de ninguna de las dos claves.

Imaginemos ahora que la clave para cifrar y la manera en que esta clave se usa para cifrar se da a conocer al público entonces es posible, para cualquiera que tenga conocimiento de los enteros módulo 26, encontrar la clave para descifrar el mensaje.

En la siguiente sección construiremos dos tipos de cifrados en los cuales la clave y la manera de como usar esta clave para cifrar se da a conocer al público. Sin embargo, veremos que aún bajo estas circunstancias, encontrar la clave para descifrar es "muy difícil". La dificultad para encontrar la clave para descifrar recae en el hecho, aún no demostrado, de que **factorizar** ó encontrar **logaritmos discretos** son problemas "muy difíciles". Mas adelante, en la sección titulada ElGamal definiremos el logaritmo discreto y basado en esto construiremos el cifrado de ElGamal.

Puede definirse con presición que quiere decir ser "muy difícil". Bástenos aquí, que difícil significa que factorizar ó encontrar logarithmos discretos toma mucho tiempo.

4. Cifrados de clave pública

4.1. RSA: R. L. Rivest, A. Shamir, and L. Adleman.

Definición 51. *Sea n un número entero positivo. Sea*

$$\Phi(n) = \{j \mid 1 \leq j \leq n-1,\ j \textit{ primo relativo con } n\}$$

Definimos $\varphi(n)$ como el número de elementos de el conjunto $\Phi(n)$.

Ejemplo 52. $\phi(2) = 1$, $\phi(5) = 4$, $\phi(8) = 4$.

Lema 53. *Sean p y q dos números primos y $n = pq$. Entonces*

$$\varphi(n) = (p-1)(q-1).$$

Demostración. Ejercicio. □

Ejercicio 54. *Si es posible, encuentre p y q tal que $\varphi(pq) = 1000$. Si existen p y q tal que $\varphi(pq) = 1000$, cuántos pares (p, q) existen con esta propiedad?*

Cifrado 55. ***RSA***. *Sea $n = pq$, p y q números primos. Sean x un elemento de $\mathbb{Z}_n$, y c, d números enteros tal que*

$$0 < c < \varphi(n),\ 0 < d < \varphi(n) \textit{ y } cd \equiv 1 \text{ mód } \varphi(n).$$

Definimos las funciones

$$cifrarRSA_c^n : \mathbb{Z}_n \to \mathbb{Z}_n \quad cifrarRSA_c^n(x) = x^c$$
$$descifrarRSA_d^n : \mathbb{Z}_n \to \mathbb{Z}_n \quad descifrarRSA_d^n(x) = x^d$$

El par (n, c) es la clave pública, $(p, q, \varphi(n))$ se mantienen en privado. El mensaje sin cifrar es x, el mensaje cifrado es x^c.

Lema 56. *Las funciones $descifrarRSA_d^n$ y $cifrarRSA_c^n$ satisfacen*

$$descifrarRSA_d^n(cifrarRSA_c^n(x)) = x.$$

Demostración. Tenemos que desmostrar que $(x^c)^d \equiv x$ mód $\varphi(n)$. Esto es, tenemos que demostrar que

$$x^{cd} \equiv x \text{ mód } \varphi(n).$$

Esto se sigue inmediatamente de el siguiente teorema. □

Teorema 57. ***EULER.*** *Sea k un numero entero positivo y x un elemento de $\mathbb{Z}_n$, entonces*

$$x^{k\varphi(n)+1} \equiv x \text{ mód } n.$$

Además, si x es primo relativo con n

$$x^{\varphi(n)} \equiv 1 \text{ mód } n.$$

Demostración. Supongamos primero que x es primo relativo con n. Sea

$$\{r_1, r_2, r_3, ..., r_{\varphi(n)}\}$$

un sistema reducido completo de representantes de las unidades de $\mathbb{Z}_n$. Como x es primo relativo con n, no es difícil cersiorarse de que

$$\{xr_1, xr_2, xr_3, ..., xr_{\varphi(n)}\}$$

es también un sistema reducido completo de representantes de las unidades de $\mathbb{Z}_n$. Se sigue que

$$r_1 \cdot r_2 \cdot r_3 \cdot \cdots \cdot r_{\varphi(n)} \equiv x \cdot r_1 \cdot x \cdot r_2 \cdot x \cdot r_3 \cdot \cdots \cdot x \cdot r_{\varphi(n)} \text{ mód } n$$

así que

$$r_1 \cdot r_2 \cdot r_3 \cdot \cdots \cdot r_{\varphi(n)} \equiv x^{\varphi(n)} \cdot r_1 \cdot r_2 \cdot r_3 \cdot \cdots \cdot r_{\varphi(n)} \text{ mód } n$$

y por lo tanto

$$x^{\varphi(n)} \equiv 1 \text{ mód } n$$

ya que $r_1 \cdot r_2 \cdot r_3 \cdot \cdots \cdot r_{\varphi(n)}$ tiene inverso multiplicativo en $\mathbb{Z}_n$. Observemos que si x es primo relativo con n entonces x^k es primo relativo con n y se sigue que

$$x^{k\varphi(n)} \equiv 1 \text{ mód } n$$

y se concluye que

$$x^{k\varphi(n)+1} \equiv x \text{ mód } n$$

Supongamos ahora que x no es primo relativo con n. Entonces p divide a x y por lo tanto p divide a $x^{k\varphi(n)+1} - x$. Si q divide a x entonces q divide a $x^{k\varphi(n)+1} - x$ y por lo tanto $n = pq$ divide a $x^{k\varphi(n)+1} - x$. Si q no divide a x entonces q no divide a $x^{k(p-1)}$ y se sigue de el pequeño teorema de Fermat, Teorema [45], que

$$x^{k(p-1)(q-1)} \equiv 1 \text{ mód } q$$

y por tanto

$$x^{k\varphi(n)+1} \equiv x \text{ mód } q,$$

esto es, q divide a $x^{k\varphi(n)+1} - x$ y de nuevo tenemos que $n = pq$ divide a $x^{k\varphi(n)+1} - x$ pues p y q son números primos. □

4.2. ElGamal. El cifrado de ElGamal esta basado en el logaritmo discreto, así que empezaremos por definir este concepto. Comenzaremos definiendo el concepto de grupo finito.

Definición 58. *Sea G un conjunto no vacío finito dotado de una operacion binaria llamada producto o multiplicación y denotada por $\cdot$. Esto es, dados dos elementos g y h en G el producto de g y h es $g \cdot h$ o simplemente gh si no existe confución. El producto debe satisfacer las propiedades siguientes*

1. La operación es cerrada: gh está en G.
2. La operación es asociativa: $(gh)k = g(hk)$.
3. Existe elemento identidad: existe e en G tal que $ge = eg = g$.
4. Existen inversos: para todo elemento g en G existe g^{inv} tal que $gg^{inv} = g^{inv}g = e$.

Ejercicio 59. *Demuestre que si e y $\overline{e}$ en G satisfacen $ge = eg = g$ y $g\overline{e} = \overline{e}g = g$ para todo g en G entonces $e = \overline{e}$. Esto es, sólo existe un elemento indentidad. Similarmente, dado g en G sólo existe un elemento g^{inv}.*

Definición 60. *El grupo G se llama Abeliano si $gh = hg$ para todo par de elementos g y h en G.*

De aquí en adelante escribiremos g^m en lugar de

$$\underbrace{g \cdot g \cdot \cdots \cdot g}_{m \text{ veces}}$$

y $g^{-m} = (g^{inv})^m$. Por convención, $g^0 = e$.

Lema 61. *Si g es un elemento de G entonces existe un número entero positivo n tal que $g^n = e$.*

Demostración. El conjunto

$$\{g, g^2, g^3, ..., g^k, ...\}$$

es finito pues esta contenido en G. Por lo tanto existen $i < j$ tal que $g^i = g^j$ y por lo tanto $g^{j-i} = e$. Tómese $n = j - i$. □

Definición 62. *Sea S el subconjunto de los números enteros positivos definido como sigue,*

$$S = \{n \mid n \text{ número entero positivo tal que } g^n = e\}$$

El orden de g denotado $ord(g)$ es el elemento mínimo de S.

Definición 63. *Sea G un grupo finito con N elementos. Decimos que G es cíclico si existe g en G tal que $ord(g) = N$.*

Lema 64. *Sea G un grupo cíclico y g un generador de G. Entonces,*

$$G = \{g, g^2, g^3, ..., g^{ord(g)}\}.$$

Demostración. Claramente

$$\{e, g, g^2, g^3, ..., g^{ord(g)-1}\} \subseteq G.$$

y contando los elementos se ve que se tiene igualdad de conjuntos. □

Definición 65. *Sea G un grupo finito y g un generedor de G. Sea h un elemento de G y m un entero positivo tal que $g^m = h$ y $0 \leq m < ord(g)$. Definimos el logaritmo discreto de h con respecto a g como m. Obsérvese que m es único.*

Lema 66. *Sea G un grupo finito y g un elemento en G. Si $g^k = e$ entonces $ord(g)$ divide a k.*

Demostración. Escribamos $k = qord(g) + r$, $0 \leq r < ord(g)$. Por hipótesis tenemos

$$e = g^k = g^{qord(g)+r} = g^{qord(g)}g^r = (g^{ord(g)})^q g^r = e^q g^r = eg^r = g^r.$$

Cómo $ord(g)$ es el menor número entero positivo con la propiedad $g^{ord(g)} = e$, r tiene que ser 0. Esto es, $k = qord(g)$ y se sigue que $ord(g)$ divide a k. □

Definición 67. *Un **campo** es un conjunto no vacío $\mathbb{F}$ dotado de dos operaciones binarias (suma, $+$) y (multiplicación, $\cdot$) tal que*

1. *$\mathbb{F}$ dotado con la suma es un grupo Abeliano. El elemento identidad de la suma es denotad por 0.*
2. *$\mathbb{F} \setminus \{0\}$ dotado con la multipliación es un grupo Abeliano. El elemento identidad de la multiplicación es denotad por 1.*
3. *Para todo a, b, c en $\mathbb{F}$, $a \cdot (b + c) = a \cdot b + a \cdot c$.*

Definición 68. *La caraterística de $\mathbb{F}$ es el menor entero positivo p tal que $p \cdot 1 = 0$. Si tal p no existe, definimos la caraterística de $\mathbb{F}$ como 0.*

Teorema 69. *Si la característica de $\mathbb{F}$ es $p > 0$ then p is prime.*

Teorema 70. *Cualquier campo finito de caraterística p tiene p^n elementos para algún entero positivo n.*

Sea $\mathbb{F}$ un campo y $\mathbb{F}^* = \{f \in \mathbb{F} \mid f \neq 0\}$.

Teorema 71. *Si $\mathbb{F}$ es un campo finito entonces $\mathbb{F}^*$ dotado de el producto como operación binaria, es un grupo cíclico.*

Demostración. Idea de la desmostración seguiendo a Emil Artin. Sean f y g dos elementos de $\mathbb{F}^*$ de orden k y l primos relativos. El elemento fg satisface $(fg)^{kl} = 1$. Entonces $ord(fg)$ divide a kl, Lema [66]. Como k y l son primos relativos se concluye que $ord(fg) = kl$. Además, si k divide a $ord(g)$ entonces $g^{ord(g)/k}$ tiene orden k. Esto es, para cualquier divisor $ord(g)$ podemos encontrar un elemento de G con ese orden.

Supongamos ahora que

$$ord(g) = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$$
$$ord(f) = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$$

Sea $t_i = \text{máx}(n_i, m_i)$ y pongamos

$$c = p_1^{t_1} p_2^{t_2} \cdots p_r^{t_r}$$

Hemos visto que podemos encontrar un elemento de h_i de orden $p_i^{t_i}$ y se sigue que el $h_1 h_2 \cdots h_r$ tiene orden c. Obsérvese que c es el mínimo común múltiplo de $ord(g)$ y $ord(f)$. Cómo $\mathbb{F}^*$ es finito, $\mathbb{F}^*$ tiene un elemento g_0 de orden máximo. De lo anterior se concluye que el orden de cualquier elemento de $\mathbb{F}^*$ divide a $ord(g_0)$. Así que todo elemento de G satisface la ecuación

$$x^{ord(g_0)} - 1 = 0.$$

Claramente $ord(g_0)$ es menor o igual que el número de elementos de $\mathbb{F}^*$. Por otro lado como el polinomio $x^{ord(g_0)} - 1$ tiene a lo sumo $ord(g_0)$ raíces y todo elemento de $\mathbb{F}^*$ es raiz de este polinomio el número de elementos de $\mathbb{F}^*$ tiene que ser menor o igual que $ord(g_0)$. Por lo tanto el número de elementos de $\mathbb{F}^*$ es $ord(g_0)$ y $\mathbb{F}^*$ es cíclico. □

Cifrado 72. ***ElGamal.*** *Sea $\mathbb{F}$ un campo finito. Supongamos que $\mathbb{F}^*$ tiene N elementos, con $N \approx 10^{100}$ y tal que N es primo ó $N = pM$ tal que $p \approx 10^{95}$ es primo. La potencia 95 no es especial sólo queremos que p sea grande. Cómo $\mathbb{F}^*$ es cíclico, existe un elemento f en $\mathbb{F}^*$ de orden pM. Por lo tanto el elemento $g = f^M$ tine orden p. Sea G el subgrupo de $\mathbb{F}^*$ generado por g. Esto es*

$$G = \{g, g^2, ..., g^{p-2}, g^p - 1, g^p = 1\}.$$

Escogemos un número entero c aleatoriamente, $0 < c < p$ y ponemos $h = g^c$. Sea x un elemento de G. y k un número entero positivo escogido aleatoriamente. Definimos las funciones

$$cifrarElG_c^p : G \to G \times G \quad cifrarElG_c^p(x) = (g^k, xh^k)$$
$$descifrarElG_c^p : G \times G \to G \quad descifrarElG_c^p(x_1, x_2) = x_2 x_1^{-c}$$

El par (g, h) es la clave pública, c se mantiene en privado. El mensaje sin cifrar es x, el mensaje cifrado es el par (g^k, xh^k).

Ejercicio 73. *Demuestre que*

$$descifrarElG_c^p(cifrarElG_c^p(x)) = x.$$

4.3. Intercambio de claves. Sea G un grupo cíclico de orden n con generador g. Supongamos que Ana y Bernardo quieren intercambiar una clave para comunicarse secretamente. Ana escoge un número a aleatoriamente, entre 1 y $n-1$ en secreto, calcula g^a y lo publica. Bernardo hace el mismo proceso, escoge un número b aleatoriamente, entre 1 y $n-1$ en secreto, calcula g^b y lo publica. Ana y Bernardo pueden calcular $g^{ab} = (g^a)^b = \left(g^b\right)^a$. Sin embargo, se cree que la única manera en que un tercero puede calcular g^{ab} es resolviendo el problema del logaritmo discreto $g^x = g^a$ and $g^y = g^b$.

4.4. Firmas digitales. Antes de explicar el protocolo para firmas digitales definiremos lo que es una función *hash*.

Definición 74. *Una función hash, es una función $h : \{0,1\}^{10^k} \to \{0,1\}^n$ con k un entero positivo entre 8 y 20 y n es un entero positivo entre 100 y 400 satisfaciendo las siguientes propiedades:*

1. *es dificil resolver la ecuación $h(x) = a$ y*
2. *es dificil encontrar x_1 y x_2 tal que $h(x_1) = h(x_2)$.*

Supongamos que Ana quiere firmar un documento digital. Ana ejecuta el siguiente procedimiento:

1. escoge un número primo q de al menos 200 bits.
2. escoge un segundo número primo p de al menos 600 bits tal que, $p \equiv 1 \bmod q$
3. escoge un generador del subgrupo cíclico $\mathbb{Z}_p^*$ de orden q. (para encontrar un generador Ana puede calcular $g^{(p-1)/q} \bmod p$ con un entero positivo aleatorio g y checar que $g^{(p-1)/q} \not\equiv 1 \bmod p$). Si esto no es así, Ana escoge un nuevo entero positivo aleatoriamente y repite el cálculo hasta encontrar un entero positivo g satisfaciendo $g^{(p-1)/q} \not\equiv 1 \bmod p$.
4. escoge un número x entre 1 y q aleatoriamente como su clave secreta y publica su clave $y = g^x \bmod p$

Para firmar un documento binario m, Ana calcula $h_0 = h(m)$, $h(m)$ debe ser un entero entre 0 y q. Despues escoge un número entero k aleatoriamente (en el mismo rango de $h(m)$), calcula $g_0 = g^k \bmod p$ y fija $r \equiv g_0 \bmod q$ con r el mínimo entero positivo que satisface esta congruencia. Finalmente, Ana encuentra un entero s tal que $sk \equiv h_0 + xr \bmod q$. Su firma es la pareja ordenada $(r, s) \in \mathbb{Z}_q^2$.
Para verificar que Ana envió el documento, Bernardo calcula $a_1 = s^{-1}h_0 \bmod q$ y $a_2 = s^{-1}r \bmod q$. Luego calcula $w = g^{a_1}y^{a_2} \bmod p$. Si $w \equiv r \bmod q$, Bernardo queda satisfecho. Nótese que

$$\left(g^{a_1}y^{a_2} \equiv g^{s^{-1}(h_0+xr)} \equiv g^k\right) \bmod p$$

4.5. Cifrados completamente homomórficos. El cifrado RSA satisface la siguiente propiedad multiplicativa. Supongamos que x_1 y x_2 son dos mensajes y que $x_1^c \bmod N$ y $x_2^c \bmod N$ son los mensajes cifrados correspondientes. Al mensaje x_1x_2 le corresponde el mensaje cifrado $(x_1x_2)^c \bmod N$. Sabemos que $(x_1x_2)^c \bmod N = x_1^c x_2^c \bmod N = (x_1^c \bmod N)((x_2^c \bmod N)$.
Sin embargo, $(x_1 + x_2)^c \bmod N \neq x_1^c + x_2^c \bmod N$ in general. Un cifrado completamente homórfico es un cifrado que respeta la multipicación y la suma. Así que RSA no es un cifrado completamente homomórfico.

La razón por la que nos gustaría construir un cifrado completamente homomórfico es que esto nos permitiría ejecutar operaciones en el cifrado de una base de datos. Esto abre las puertas para analizar base de datos sin comprometer la confidencialidad.

5. Códigos correctores de errores

Los sistemas de comunicación así cómo los almacenes de datos no son cien por ciento confiables pues son sujetos a errores causados por interferencias. El propósito de los códigos correctores de errores es dectectar y tratar de corregir estos errores a como uno va. En este capítulo veremos como construir varios tipos de códigos capaces de detectar y corregir errores. Empezaremos por definir códigos binarios, despues definiremos códigos lineales, estos últimos son códigos con estructura de espacio vectorial y finalmente definiremos códigos lineales no binarios.

5.1. Códigos binarios.

Definición 75. *Un código C es un conjunto de palabras formadas usando símbolos de un conjunto fijo A llamado alfabeto. En general, A es un conjunto finito.*

Definición 76. *Un código binario C usa como alfabeto el campo $\mathbb{Z}_2 = \{0, 1\}$.*

De aquí en adelante nuestro alfabeto será siempre un campo finito $\mathbb{F}$.

Definición 77. *C es un código de bloque de longitud n si toda palabra w de C tiene longitud n. Esto es, w se escribe usando n símbolos de el alfabeto.*

Ejemplo 78. *El código C definido abajo es un código binario de bloque de longitud 3 que contiene 4 palabras.*

$$C = \{001, 100, 000, 010\}$$

Ejemplo 79. *Sea $\mathbb{Z}_5$ nuestro alfabeto. El código C definido abajo es un código no-binario de bloque de longitud 4 que contiene 3 palabras.*

$$C = \{0201, 000, 3214\}$$

Definición 80. *Sea w una palabra en el código C. El peso de w, denotado peso(w), es el número de símbolos distintos de cero que aparecen en w. Por ejemplo, la palabra* 3214 *satisface peso*$(3214) = 4$ *mientras que para* 0201 *tenemos peso*$(0201) = 2$.

Definición 81. *Sea C un código de bloque de longitud n y w_1, w_2 dos palabras en C.*

$$w_1 = w_{11}w_{12}...w_{1n}$$
$$w_2 = w_{21}w_{22}...w_{2n}$$

la distancia entre w_1 y w_2, denotada $d(w_1, w_2)$, se define cómo la cardinalidad de el conjunto

$$D = \{i \text{ tal que } w_{1i} \neq w_{2i}\}$$

Ejercicio 82. ***Desigualdad de el triángulo.*** *Sea C un código de bloque y w_1, w_2, w_3, tres palabras en C. Demuestre que*

$$d(w_1, w_2) \leq d(w_1, w_3) + d(w_3, w_2)$$

Definición 83. *Sea C un código de bloque. Definimos la distancia mínima de C, denotada $d_{\text{mín}}$, cómo:*

$$d_{\text{mín}} = \text{mín}\{d(w_i, w_j) \mid (w_i, w_j) \in C \times C, w_i \neq w_j\}$$

5.2. Códigos lineales. Sea $\mathbb{F}$ un campo. Comenzamos definiendo algunos términos de álgebra lineal.

Definición 84. *Un conjunto no vacío V es un espacio vectorial sobre $\mathbb{F}$ si y sólo si existen dos operaciones*

$$+: \quad V \times V \to V$$
$$\cdot: \quad \mathbb{F} \times V \to V$$

satisfaciendo la siguientes propiedades. Para todo u, v, w en V y α, β en $\mathbb{F}$

1. $u + v = v + u$
2. $(u + v) + w = u + (v + w)$
3. Existe un elemento $\vec{0}$ en V, tal que $\vec{0} + v = v + \vec{0} = v$
4. Para todo elemento v en V existe un elemento ${}_{menos}v$ tal que
$${}_{menos}v + v = v +_{menos} v = \vec{0}$$
5. $\alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v$
6. $(\alpha + \beta) \cdot v = \alpha \cdot v + \beta \cdot v$
7. $(\alpha\beta) \cdot v = \alpha(\beta \cdot v)$
8. $1 \cdot v = v$

Definición 85. *Sea V un espacio vectorial sobre $\mathbb{F}$ y W un sobconjunto de V. Decimos que W es un subespacio vectorial de V si y sólo si W satisface*

1. $u + v$ está en W para todo u, v en W
2. $\alpha \cdot v$ está en W para toda α en $\mathbb{F}$ y toda v en W

Nótese que un subespacio vectorial es un espacio vectorial cundo lo pensamos por si solo.

Ejercicio 86. *Sea $\mathbb{F}^n$ el conjunto*

$$\mathbb{F}^n = \underbrace{\mathbb{F} \times \mathbb{F} \times \cdots \times \mathbb{F} \times \mathbb{F}}_{n\text{times}}.$$

Definimos

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = \quad (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$
$$\alpha \cdot (a_1, a_2, \ldots, a_n) = \quad (\alpha \cdot a_1, \alpha \cdot a_2, \ldots, \alpha \cdot a_n)$$

Demuestre que $\mathbb{F}^n$ con estas dos operaciones es un espacio vectorial sobre $\mathbb{F}$.

De aquí en adelante identificaremos las palabras de longitud n con elementos de $\mathbb{F}^n$. De esta manera un código de bloque C de longitud n puede considerarse como un subconjunto de $\mathbb{F}^n$.

Definición 87. *Un código de bloque C de longitud n es un código lineal si C es un subespacio vectorial de $\mathbb{F}^n$.*

Definición 88. *Sean $v_1, v_2, \ldots, v_k$ elementos de un espacio vectorial V sobre $\mathbb{F}$. Una combinación lineal de $v_1, v_2, \ldots, v_k$ con coeficientes en $\mathbb{F}$ es una expresión de la forma*

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k$$

con $\alpha_1, \alpha_2, \ldots, \alpha_k$ elementos de $\mathbb{F}$.

Ejercicio 89. *Sean $v_1, v_2, \ldots, v_k$ elementos de un espacio vectorial V sobre $\mathbb{F}$. Demuestre que el conjunto de todas las combinaciones lineales de $v_1, v_2, \ldots, v_k$ con coeficientes en $\mathbb{F}$ es un subespacio vectorial de V.*

Definición 90. *El subespacio vectorial en el ejercicio anterior es llamado el subespacio generado por $v_1, v_2, \ldots, v_k$.*

Definición 91. *Sean $v_1, v_2, \ldots, v_k$ elementos de un espacio vectorial V sobre $\mathbb{F}$. Diremos que $v_1, v_2, \ldots, v_k$ son linealmente independientes si cada vez que tenemos*

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k = \vec{0} \in V$$

entonces $\alpha_1 = \alpha_2 = \cdots = \alpha_k = 0 \in \mathbb{F}$. Si $v_1, v_2, \ldots, v_k$ no son linealmente independientes diremos que son linealmene dependientes. Esto es, existe una combinación lineal

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k = \vec{0} \in V$$

con algún α_i distinto de 0.

Definición 92. *Sea W un subespacio vectorial de el espacio vectorial V. Sean $w_1, w_2, \ldots, w_k$ elementos de W. Diremos que el conjunto $\{w_1, w_2, \ldots, w_k\}$ es una base de W si $w_1, w_2, \ldots, w_k$ son linealmente independientes y W es igual al subespacio vectorial generado por $w_1, w_2, \ldots, w_k$.*

Teorema 93. *Sea W un subespacio vectorial de V. Si W tiene una base con k elementos entonces cualquier otra base de W tiene también k elementos.*

Demostración. La demostración se dará em el curso. □

Definición 94. *Sea W un subespacio vectorial de V. Si $w_1, w_2, \ldots, w_k$ es una base de W, definimos la dimensión de W como el entero positivo k. En este caso diremos que W tiene dimensión k. Se sigue de el teorema anterior que la dimension está bien definida.*

Definición 95. *Un código lineal de bloque C de longitud n es un código de tipo $[n, k]$ si C tiene dimensión k.*

Ejemplo 96. *Un código C_1 lineal binario de tipo $[3, 2]$.*

$$C_1 = \{000, 001, 100, 101\}$$

Ejemplo 97. *Un código C_2 lineal binario de tipo $[7, 4]$.*

0000000	0100101	1000110	1100101
0001111	0101100	1001001	1101010
0010101	0110110	1010011	1110000
0011010	0111001	1011100	1111111

El código C_2 es un subspacio vecotorial de $\mathbb{Z}_2^7$. Sean H y G las matrices

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \quad \textit{and} \quad G = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

La matriz G define una transformación lineal $G : \mathbb{Z}_2^4 \to \mathbb{Z}_2^7$ cuya imagen es C_2. La matriz H define una tranformación lineal $H : \mathbb{Z}_2^7 \to \mathbb{Z}_2^3$ cuyo núcleo es C_2. Sean $v_1 = (1,0,0,0,0,0,0)$, $v_2 = (0,1,0,0,0,0,0)$, ..., $v_6 = (0,0,0,0,0,1,0)$,$v_7 = (0,0,0,0,0,0,1)$, vectores en $\mathbb{Z}_2^7$. Pongamos $w_i = Hv_i$.

$$w_1 = (1,1,0) \qquad w_5 = (1,0,0)$$
$$w_2 = (0,1,1) \qquad w_6 = (0,1,0)$$
$$w_3 = (1,0,1) \qquad w_7 = (0,0,1)$$
$$w_4 = (1,1,1)$$

Sea v un elemento de $\mathbb{Z}_2^7$ que no está en C_2. Existe una única $1 \leq i \leq 7$, tal que $Hv = w = Hv_i$. (v_i se denomina el sindrome de v.) Cómo $H(v - v_i) = (0,0,0)$, existe una única c en C_2 tal que $v = v_i + c$.

Ejemplo 98. *Un codigo C_3 lineal no-binario de tipo $[3,2]$ con alfabeto $\mathbb{Z}_3$.*

$$C_3 = \{000, 101, 010, 111, 202, 020, 222, 212, 121\}$$

Definición 99. *Sea C un código de tipo $[n,k]$. Decimos que C es un código de tipo $[n,k,d]$ si C tiene distancia mínima d.*

El código C_1 es un código $[3,2,1]$, C_2 es un código $[7,4,3]$ y C_3 es de tipo $[3,2,1]$.

Ejercicio 100. *Corrobore que $\{001, 100\}$ es una base de C_1 y que*

$$\{1000110, 0100011, 0010101, 0001111\}$$

es una base de C_2. Encuentre una base de C_3.

Definición 101. *La rapidez de un código de tipo $[n,k]$ se define como k/n.*

Lema 102. *Sea C un código de tipo $[n,k,d]$. Entonces, C puede detectar $d-1$ errores y corregir de 1 a $(d-1)/2$ errores.*

Lo que este lema dice es que si a lo sumo $d-1$ símbolos de una palabra w de C son modificados para obtener una palabra $\widehat{w}$ entonces uno sabe con cien por ciento de certeza que $\widehat{w}$ no está en C. Además, si $(d-1)/2$ símbolos o menos de w son modificados para obtener $\widehat{w}$ entonces la única palabra de C que al modificarse $(d-1)/2$ o menos símbolos y que da lugar a $\widehat{w}$ es w. Esto es, w es la única palabra de C tal que $d(w,\widehat{w}) \leq (d-1)/2$.

Demostración. Supongamos que $d(w,\widehat{w}) \leq (d-1)$. Si $\widehat{w}$ es un elemento de C entonces la distancia mínima de C es menor o igual que $d-1$. Esto contradice que la distancia mínima de C es d. Así que C detecta de 1 a $d-1$ errores.

Supongamos ahora que existen w y w' en C tal que

$$d(w,\widehat{w}) \leq (d-1)/2 \text{ y } d(w',\widehat{w}) \leq (d-1)/2$$

y que d es impar. Sea $d = 2t+1$. Entonces, $(d-1)/2 = t$

$$d(w,w') \leq d(w,\widehat{w}) + d(w',\widehat{w}) \leq (d-1)/2 + (d-1)/2 = t + t = 2t < d,$$

por la desigualdad de el triángulo. Esto implica que la distancia mínima de C es menor que d. Lo cual es una contradicción. El caso en que d es par se deja como ejercicio. □

Lema 103. *Sea C un código lineal de bloque de tipo $[n,k,d]$ y q el número de elementos de $\mathbb{F}$, entonces C tiene q^k palabras.*

Demostración. Cómo C tiene dimensión k, existen $w_1, w_2, \ldots, w_k$ que son una base de C. Obsérvese que cada elemento de C se representa de manera única como combinación lineal de los $w_1, w_2, \ldots, w_k$. Es decir si w está en C entonces

$$w = \alpha_1 w_1 + \alpha_2 w_2 + \cdots + \alpha_k w_k$$

con $\alpha_1, \alpha_2, \ldots, \alpha_k$ en $\mathbb{F}$ únicos con respecto a w. Esto quiere decir que podemos construir $\underbrace{q \cdot q \cdot q \cdots q}_{k \text{ veces}}$ palabras.

Esto es C tiene q^k palabras. □

Lema 104 (Cota de Singleton)**.** *Sea C un código lineal de bloque de tipo $[n, k, d]$, entonces $k + d \leq n + 1$.*

Demostración. Sabemos que $d \leq n$. Sea C' el conjunto de palabras de longitud $n-d+1$ que se obtiene borrando los últimos $d-1$ símbolos de cada palabra en C. Todas las palabras en C' son distintas porque la distancia mínima de C es d. De manera similar al lema anterior uno ve que el número de palabras en C' es menor o igual que q^{n-d+1}. Cómo C tiene q^k palabras y la función $w \to w'$, de C en C', es inyectiva, se tiene que $q^k \leq q^{n-d+1}$. Esto implica que $k \leq n - d + 1$, lo cual es equivalente a

$$k + d \leq n + 1.$$

□

Definición 105. *Un código C de tipo $[n, k, d]$ tal que $k + d = n + 1$ se le llama de distancia máxima separable o simplemente DMS.*

Ejercicio 106. *Para que pares $[k, d]$ $k > 1$, existen códigos binarios lineales de tipo $[6, k, d]$ que son DMS?*

5.3. Códigos no binarios.

5.3.1. Códigos de Reed-Solomon. Los códigos de Reed-Solomon son una clase muy importante de códigos no-binarios. Se usan en la codificación de música digital por ejemplo. La construcción de estos códigos es aparentemente simple sin embargo es bastante sofisticada. Empezamos con algunas definiciones.

Definición 107. *Sea $\mathbb{F}$ nuestro campo finito con q elementos y $\mathbb{F}[x]$ el anillo de polinomios en x.*

$$\mathbb{F}[x] = \{p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n | a_i \text{ en } \mathbb{F},\ a_n \neq 0 \text{ y } a_{n+i} = 0 \text{ para todo entero positivo } i\}.$$

Sean $p_1(x)$ y $p_2(x)$ dos polinomios en $\mathbb{F}[x]$,

$$p_1(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

$$p_2(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n$$

Aqui estamos suponiendo $a_n \neq 0$, $a_k = b_k = 0$ para $k > n$, y b_n pudiera ser 0. La suma $p_1(x) + p_2(x)$ es el polinomio

$$(a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots + (a_n + b_n)x^n.$$

El producto $p_1(x) \cdot p_2(x)$ es el polinomio

$$c_0 + c_1x + c_2x^2 + \cdots + c_{2n}x^{2n}$$

con

$$c_i = a_ib_0 + a_{i-1}b_1 + \cdots + a_0b_i$$

para $0 \leq i \leq 2n$. Nótese que c_{2n} pudiese ser 0.

Ejercicio 108. *Demuestre que $\mathbb{F}[x]$ dotado de las operaciones suma y producto definidades anteriormente es un dominio entero.*

Definición 109. *Sea $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ con $a_n \neq 0$. El grado de $p(x)$ se define como n.*

Sea $k < q - 1$ y $P_k(x)$ el conjunto de polinomios de grado menor que k,

$$P_k(x) = \{p(x) \mid p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{k-1}x^{k-1}\}.$$

Sea

$$\mathbb{F}^* = \{\alpha_1, \alpha_2, \ldots, \alpha_{q-1}\}$$

$\alpha_i \neq 0$, $\alpha_i \neq \alpha_j$ para $i \neq j$ and $i = 1, 2, \ldots, q-1$. $\mathbb{F}^*$ consiste de todos los elementos de $\mathbb{F}$ distintos de 0.

Algoritmo 110 (Algoritmo de la división)**.** *Sean $f(x)$ y $h(x)$ dos elementos de $\mathbb{F}[x]$ con $h(x) \neq 0$. Entonces existen dos polinomios en $\mathbb{F}[x]$, $q(x)$ y $r(x)$ únicos tal que*

$$f(x) = q(x)h(x) + r(x),$$

con $r(x)$ el polinomio cero ó grado de $r(x)$ estrictamente menor que el grado de $h(x)$. El polinomio $q(x)$ se llama el cociente y el polinomio $r(x)$ se llama el residuo.

A el polinomio $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-2}x^{n-2} + a_{n-1}x^{n-1}$ de grado menor ó igual que $n-1$ en $\mathbb{F}[x]$ le asociaremos de manera única la palabra de longitud n, $(a_0a_1a_2 \ldots a_{n-2}a_{n-1})$. Se sigue que dado un código lineal C de longitud n sobre $\mathbb{F}$, C puede identificarse con el espacio vectorial de polinomios de grado menor ó igual que $n-1$ en $\mathbb{F}[x]$. Este último espacio vectorial tiene dimensión n.

Definición 111. *Sean $f_1(x)$, $f_2(x)$ y $h(x)$ polinomios en $\mathbb{F}[x]$. Decimos que $f_1(x)$ y $f_2(x)$ son equivalentes ó congruentes módulo $h(x)$ si y sólo si $f_2(x) - f_1(x) = q(x)h(x)$.*

Ejercicio 112. *Demuéstrese que esta es una relación de equivalencia. Usaremos la siguiente notación:*

$$f(x) \equiv g(x) \bmod h(x)$$

para denotar esta relación.

Lema 113. *Si $f(x) \equiv g(x) \bmod h(x)$ entonces*

1. *$f(x) + p(x) \equiv g(x) + p(x) \bmod h(x)$ y*
2. *$f(x)p(x) \equiv g(x)p(x) \bmod h(x)$.*

Demostración. Ejercicio. □

Definición 114. *Sea $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ con $a_n \neq 0$ un polinomio. Un elemento α de $\mathbb{F}$ es una raíz de $p(x)$ si $p(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0$.*

Teorema 115. ***Número de raices.*** *Sea $p(x)$ un elemento de grado n entonces $p(x)$ tiene a lo sumo n raices.*

Demostración. La demostración se deja como problema. Sólo se requiere de el algoritmo de la división de polinomios y de que el grado de el producto es la suma de los grados. □

Definición 116. *Sea $p(a)$ un polinomio irreducible de grado r en $\mathbb{Z}_2[a]$ y $\mathbb{F} = \mathbb{Z}_2[a]/\langle p(a)\rangle$. El polinomio $p(a)$ es primitivo si y sólo si*

$$\mathbb{F}^* = \left\{a,\, a^2, \ldots, a^{2^r-2},\, a^{2^r-1} = 1\right\}.$$

Para construir los códigos de Reed-Solomon empezamos por escoger un polinomio primitivo $p(a)$ de grado n en $\mathbb{Z}_2[a]$ y construinos el campo finito $\mathbb{F}_{2^n} = \mathbb{Z}_2[a]/p(a)$ con 2^n elementos. Las palabras de el código de Reed-Solomon son de longitud $m = 2^n - 1$ y serán identificadas con polinomios en $\mathbb{F}_{2^n}[x]$ de grado menor ó igual que $m-1$. Para construir un código de Reed-Solomon C que corrija t-errores usaremos un polinomio generador $g(x) \in \mathbb{F}_{2^n}[x]$ de la forma $g(x) = (x-a)\left(x-a^2\right)\cdots(x-a^{2t})$. La palabras en C serán múltiplos $b(x)g(x)$ de grado menor ó igual que $m-1$, con $b(x) \in \mathbb{F}[x]$. Tenemos la siguiente correspondencia:

$$\begin{array}{lcl} \text{Polinomios en } \mathbb{F}[x] & \longleftrightarrow & \text{Palabras en } \mathbb{F}^m \\ c_0 + c_1x + c_2x^2 + \cdots + c_{m-1}x^{m-1} & \longleftrightarrow & [c_0, c_1, c_2, \ldots, c_{m-1}] \end{array}.$$

Llamaremos a C un código $RS(2^n-1, t)$.

Teorema 117. *Sea $\mathbb{F}$ el campo de cardinalidad 2^n, y sea C un código $RS(2^n-1,t)$ en $\mathbb{F}[x]$. Supongamos que $c(x) \in \mathbb{F}[x]$ tiene grado menor que 2^n-1. Entonces $c(x) \in C$ si y sólo si $c(a^i) = 0$ para $i = 1, \ldots, 2t$.*

Demostración. Si $c(x) \in C$, entonces

$$c\left(a^i\right) = (a^i - a)(a^i - a^2)\cdots(a^i - a^i)\cdots(a^i - a^{2t}) = 0$$

ya que $(a^i - a^i) = 0$. Si $c(a^i) = 0$ para $i = 1, \ldots, 2t$, entonces $c(a) = 0$, lo que implica que

$$c(x) = (x-a)\cdot g_1(x).$$

Como $c(a^2) = 0 \Longrightarrow (a^2 - a)\cdot g_1(a^2) = 0$. Como $a^2 - a \neq 0$, $g_1(a^2) = 0$ así que $g_1(x) = (x-a^2)\cdot g_2(x)$. Substituyendo $g_1(x)$ en $c(x)$ obtenemos $c(x) = (x-a)(x-a^2)\cdot g_2(x)$. Continuando este proceso hasta $c(a^{2t}) = 0$ se obtiene que

$$c(x) = (x-a)(x-a^2)\cdots(x-a^{2t})\cdot g_{2t}(x)$$

el cual está en C. □

Teorema 118. *Si C es un $RS(2^n-1,t)$ entonces C corrige t-errores.*

Demostración. Sea $m = 2^n - 1$. Se sigue de el teorema anterior que si $c(x)$ es una palabra en el código de Reed-Solomon si sólo si $c(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{m-1}x^{m-1}$ y $c(a^i) = 0$ para $i = 1, 2, \ldots, 2t$. Esto implica que $c_0 + c_1a^i + c_2(a^i)^2 + \cdots + c_n(a^i)^n = 0$ para $i = 1, 2, \ldots, 2t$. Como $c_0 + c_1a^i + c_2(a^i)^2 + \cdots + c_n(a^i)^n$ es igual al producto punto de los vectores $(c_0, c_1, c_2, \ldots, , c_n)$ and $(1, a^i, a^{2i}, \ldots, a^{ni})$, se sigue que la siguiente matriz H es una matriz de paridad para C.

$$H = \begin{bmatrix} 1 & a & a^2 & \cdots & a^{m-1} \\ 1 & a^2 & \left(a^2\right)^2 & \cdots & \left(a^2\right)^{m-1} \\ 1 & a^3 & \left(a^3\right)^2 & \cdots & \left(a^3\right)^{m-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a^{2t} & \left(a^{2t}\right)^2 & \cdots & \left(a^{2t}\right)^{m-1} \end{bmatrix}$$

Demostraremos que el mínimo número de columnas linealmente dependientes de la matriz H es $2t + 1$. Primero mostraremos que cualesquier conjunto de $2t$ columnas en H tienen que ser linealmente independientes. Escojamos enteros $0 \leq j_1 \leq j_2 \leq \cdots \leq j_{2t} < m$. Las columnas de H forman la siguiente $2t \times 2t$ matriz.

$$\begin{bmatrix} a^{j_1} & a^{j_2} & \cdots & a^{j_{2t}} \\ \left(a^2\right)^{j_1} & \left(a^2\right)^{j_2} & \cdots & \left(a^2\right)^{j_{2t}} \\ \vdots & \vdots & & \vdots \\ \left(a^{2t}\right)^{j_1} & \left(a^{2t}\right)^{j_2} & \cdots & \left(a^{2t}\right)^{j_{2t}} \end{bmatrix}$$

El determinante de esta matriz puede escribirse de la forma

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ a^{j_1} & a^{j_2} & \cdots & a^{j_{2t}} \\ \vdots & \vdots & & \vdots \\ (a^{j_1})^{2t-1} & (a^{j_2})^{2t-1} & \cdots & (a^{j_{2t}})^{2t-1} \end{vmatrix} \cdot a^{j_1}a^{j_2} \cdots a^{j_{2t}},$$

el cual es distinto de cero pues es el determinante de una matriz de Vandermonde con columnas distintas. Por lo tanto, cualesquiera $2t$ columnas en H son linealmente independientes. Ademas, como H tiene $2t$ renglones, se concluye que cualesquier conjunto de $2t + 1$ columnas en H es linealmente dependiente. Es decir, el mínimo número de columnas linealmente dependientes en H es $2t+1$. Esto implica que la distancia mínimin C es $2t+1$. Por lo tanto, C es us código corrector de t-errores. □

Teorema 119. *El código C es un espacio vectorial de dimension $2^n - 1 - 2t$.*

Demostración. Los polinomios de grado menor que $2^n - 1 - 2t$ forman un espacio vectorial V de dimension $2^n - 1 - 2t$. C is isomorfo a V a través de la transformación lineal

$$\begin{array}{ccc} V & \to & C \\ v(x) & \mapsto & g(x)v(x) \end{array}$$

de esto se concluye el teorema. □

5.3.2. Algoritmo para decodificar. Sea $r(x)$ una palabra recibida con error $e(x)$. Es decir $r(x) = c(x) + e(x)$. Supongamos que $e(x)$ tiene coeficientes $e_{i_1}, e_{i_2}, .., e_{i_p}$, distintos de cero, con $p \leq t$. Fijemos

$$\begin{array}{ll} \alpha_k = a^{i_k} & \text{localizador de la posicion de el error} \\ b_k = e_{i_k} & \text{evaluador de el error} \end{array}$$

Es suficiente que determinemos los $2p$ elementos α_k, $1 \leq k \leq p$ y b_k, $1 \leq k \leq p$. Sabríamos la posición de los errores

$$e_i \neq 0 \text{ si y sólo si } a^i \text{ es uno de los } \alpha_k, 1 \leq k \leq p,$$

y si $e_i \neq 0$ entonces el error $e_i = b_k$ si y sólo si $a^i = \alpha_k$. Esto es:

$$e_i = \begin{cases} b_k & \text{si } a^i = \alpha_k \\ 0 & \text{si } a^i \neq \alpha_k \text{ para } 1 \leq k \leq p. \end{cases}$$

Para determinar α_k, es suficiente determinar el polinomio:

$$\text{localizador}(z) = (1-\alpha_1 z)(1-\alpha_2 z)\cdots(1-\alpha_p z)$$

cuyas raíces son $\alpha_1^{-1}, \alpha_2^{-1}, \ldots, \alpha_p^{-1}$, y si $\alpha_j^{-1} = a^i$ entonces $\alpha_j = a^{-i} = a^{2^n-1-i}$. Los ceros de localizador(z) se pueden encontrar evaluando este polinomio en los $2^n - 1$ elementos de el campo finito y tomar sólo aquellos en los que se anula.

Una vez que la posición de los errores ha sido determinada, el valor de los errores puede evaluarse determinando el siguiente polinomio.

$$\text{evaluador}(z) = \sum_{k=1}^{p} b_k\ \alpha_k \frac{\text{localizador}(z)}{(1-\alpha_k z)}\ = \sum_{k=1}^{p} b_k \alpha_k (1-\alpha_1 z)\cdots(1-\alpha_{k-1}z)(1-\alpha_{k+1}z)\cdots(1-\alpha_p z)\ .$$

Proposition 120. *El valor de los errores están dados por*

$$b_j = -\frac{\text{evaluador}(\alpha_j^{-1})}{\text{localizador}'(\alpha_j^{-1})}$$

donde localizador$'(z)$ *es la derivada formal de* localizador(z).

Demostración. Es claro que

$$\begin{aligned}\text{evaluador}(\alpha_j^{-1}) &= \sum_{k=1}^{p} b_k\alpha_k(1-\alpha_1\alpha_j^{-1})\cdots(1-\alpha_{k-1}\alpha_j^{-1})(1-\alpha_{k+1}\alpha_j^{-1})\cdots(1-\alpha_p\alpha_j^{-1}) \\ &= b_j\alpha_j(1-\alpha_1\alpha_j^{-1})\cdots(1-\alpha_{j-1}\alpha_j^{-1})(1-\alpha_{j+1}\alpha_j^{-1})\cdots(1-\alpha_p\alpha_j^{-1})\end{aligned}$$

por otro lado

$$\frac{d}{dz}\,\text{localizador}(z) = \sum_{k=1}^{p} -\alpha_k(1-\alpha_1 z)\cdots(1-\alpha_{k-1}z)(1-\alpha_{k+1}z)\cdots(1-\alpha_p z)$$

así que

$$\text{localizador}'(\alpha_j^{-1}) = -\alpha_j(1-\alpha_1\alpha_j^{-1})\cdots(1-\alpha_{j-1}\alpha_j^{-1})(1-\alpha_{j+1}\alpha_j^{-1})\cdots(1-\alpha_p\alpha_j^{-1}).$$

Dividiendo obtenemos

$$\frac{\text{evaluador}(\alpha_j^{-1})}{\text{localizador}'(\alpha_j^{-1})} = \frac{b_j\alpha_j(1-\alpha_1\alpha_j^{-1})\cdots(1-\alpha_{j-1}\alpha_j^{-1})(1-\alpha_{j+1}\alpha_j^{-1})\cdots(1-\alpha_p\alpha_j^{-1})}{-\alpha_j(1-\alpha_1\alpha_j^{-1})\cdots(1-\alpha_{j-1}\alpha_j^{-1})(1-\alpha_{j+1}\alpha_j^{-1})\cdots(1-\alpha_p\alpha_j^{-1})} = -b_j$$

y se sigue que

$$b_j = -\frac{\text{evaluador}(\alpha_j^{-1})}{\text{localizador}'(\alpha_j^{-1})}.$$

□

Definición 121. *El polinomio síndrome $S(z)$ se define como*

$$S(z) = S_1 + S_2 z + S_3 z^2 + \cdots + S_{2t} z^{2t-1}$$

donde $S_i = r(a^i) = e(a^i)$.

Teorema 122. *Se tienen las siguientes afirmaciones*

1. evaluador(z) = localizador$(z)S(z)$ mod z^{2t}, esto es localizador$(z)S(z) + U(z)z^{2t}$ = evaluador(z) para algún polinomio $U(z)$.
2. evaluador(z) tiene grado menor que t, y localizador(z) tiene grado a lo sumo igual a t.
3. $S(z) \neq 0$ mod z^t, esto es $S_k \neq 0$ para algún $k < t$.

Demostración. 1. Cómo $e(x) = e_{i_1}x^{i_1} + e_{i_2}x^{i_2} + \cdots + e_{i_p}x^{i_p}$ tenemos

$$e(a^i) = e_{i_1}a^{ii_1} + e_{i_2}a^{ii_2} + \cdots + e_{i_p}a^{ii_p},$$

Cómo $\alpha_k = a^{i_k}$ y $S_k = e(a^k)$ se sigue qye

$$S_i = e(a^i) = e_{i_1}\alpha_1^i + e_{i_2}\alpha_2^i + \cdots + e_{i_p}\alpha_p^i.$$

Observemos que

$$\frac{1}{1-\alpha_k z} = 1 + \alpha_k z + (\alpha_k z)^2 + (\alpha_k z)^3 + \cdots$$

entonces

$$b_k\alpha_k \frac{\text{localizador}(z)}{1-\alpha_k z} = b_k\alpha_k \,\text{localizador}(z)(1 + \alpha_k z + (\alpha_k z)^2 + (\alpha_k z)^3 + \cdots).$$

Por lo tanto,

$$\begin{aligned}
\text{evaluador}(z) &= \sum_{k=1}^{p} b_k\ \alpha_k \frac{\text{localizador}(z)}{(1-\alpha_k z)} \\
&= \sum_{k=1}^{p} b_k\alpha_k \,\text{localizador}(z)(1 + \alpha_k z + (\alpha_k z)^2 + (\alpha_k z)^3 + \cdots) \\
&= \text{localizador}(z) \sum_{k=1}^{p} b_k\alpha_k(1 + \alpha_k z + (\alpha_k z)^2 + (\alpha_k z)^3 + \cdots) \\
&= \text{localizador}(z)\left(\sum_{k=1}^{p} b_k\alpha_k + \left(\sum_{k=1}^{p} b_k\alpha_k^2\right) z + \left(\sum_{k=1}^{p} b_k\alpha_k^3\right) z^2 + \left(\sum_{k=1}^{p} b_k\alpha_k^4\right) z^3 + \cdots\right) \\
&= \text{localizador}(z)(S_1 + S_2 z + S_3 z^2 + S_4 z^3 + \cdots)
\end{aligned}$$

Esto muestra que evaluador(z) y localizador$(z)S(z)$ tienen los mismos coeficientes hasta grado $2t-1$. Esto demuestra la afirmación.

2. Esto se sigue de la definición ya que $p \leq t$.
3. Supongamos que $S_1 = S_2 = S_3 = \cdots = S_t = 0$. Esto implica que

$$\begin{aligned}
b_1\alpha_1 + b_2\alpha_2 + \cdots + b_p\alpha_p &= 0 \\
b_1\alpha_1^2 + b_2\alpha_2^2 + \cdots + b_p\alpha_p^2 &= 0 \\
&\vdots \\
b_1\alpha_1^p + b_2\alpha_2^p + \cdots + b_p\alpha_p^p &= 0
\end{aligned}$$

lo cual es equivalente a

$$\begin{bmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_p \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_p^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^p & \alpha_2^p & \cdots & \alpha_p^p \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_p \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Como esta matriz es una matriz de Vandermonde su determinante es distinto de cero, así que la única solución de el sistema es la solución trivial. Sin embargo sabemos que al menos uno de los b_i es distinto de cero. Esto es una contradicción.

□

Teorema 123. *Supongamos que $VS + Uz^{2t} = R$ para algún polinomio síndrome S, y sean V_0, U_0, y R_0 polinomios que satisfacen*

$$V_0S + U_0z^{2t} = R_0,\ \ \deg(V_0) \leq t,\ \ \deg(U_0) < t,\ \ \deg(R_0) < t.$$

Entonces existe un polinomio $h \in \mathbb{F}[z]$ tal que $V_0 = hV$, $U_0 = hU$, y $R_0 = hR$. Si también se tiene que $(V_0, U_0) = 1$, entonces h es una constante.

Demostración. Nótese que $VS + Uz^{2t} = R$ y $V_0S + U_0z^{2t} = R_0$, se sigue que

$$V_0VS + V_0Uz^{2t} = V_0R$$

y

$$VV_0S + VU_0z^{2t} = VR_0.$$

Restando estas dos igualdades se obtiene

$$(V_0U - VU_0)z^{2t} = V_0R - VR_0.$$

Comparando grados vemos que los dos lados de la ecuación tienen que ser cero. Entonces,

$$V_0U - VU_0 = V_0R - VR_0 = 0.$$

Como $(V, U) = 1$, tienen que existir polinomios $\alpha, \beta \in \mathbb{F}[z]$ tal que $\alpha V + \beta U = 1$. Por lo tanto,

$$V_0\alpha V + V_0\beta U = V_0.$$

Pero cómo $V_0U = VU_0$, entonces

$$V_0\alpha V + V\beta U_0 = V_0,$$

ó

$$(V_0\alpha + \beta U_0)V = V_0.$$

Sea

$$h = V_0\alpha + U_0\beta.$$

Entonces $hV = V_0$. Además, $hVU = V_0U = VU_0$ implica que $hU = U_0$, y $hVR = V_0R = VR_0$ implica que $hR = R_0$. Finalmente, como h tiene que dividir a V_0 y U_0, si $(V_0, U_0) = 1$, h tiene que ser una constante. □

Algoritmo 124. *El algoritmo Euclideano extendido para los enteros. Este es el algoritmo para calcular el máximo común divisor d de dos enteros a y b y los enteros u y v que satisfacen $ua + vb = d$. (Este algoritmo se generaliza para $a(x), b(x), u(x)$, y $v(x)$ en $\mathbb{F}[x]$.) Supongamos que a es mayor que b y que b positivo. (Para polinomios, supongamos que $a(x)$ tiene grado mayor que $b(x)$.)*

$a = bq_1 + r_1$	$(r_1 < b)$	*dividimos a por b con residuo r_1*
$b = r_1q_2 + r_2$	$(r_2 < r_1)$	*dividimos b por $r_1$con residuo r_2*
$r_1 = r_2q_3 + r_3$	$(r_3 < r_2)$	*dividimos r_1 por r_2 con residuo r_3*
$\vdots$	$\vdots$	$\vdots$
$r_{n-2} = r_{n-1}q_n + r_n$	$(r_n < r_{n-1})$	*dividimos r_{n-2} por r_{n-1} con residuo r_n*
$r_{n-1} = r_nq_{n+1} + 0$		*r_n es el máximo común divisor de a y b.*

Para determinar u y v, usamos la siguiente tabla y ecuaciones:

-1	$-$	$r_{-1} = a$	$u_{-1} = 1$	$v_{-1} = 0$
0	$-$	$r_0 = b$	$u_0 = 0$	$v_0 = 1$
1	q_1	r_1	u_1	v_1
2	q_2	r_2	u_2	v_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
n	q_n	r_n	u_n	v_n

donde

$$r_j = r_{j-2} - r_{j-1}q_j$$
$$u_j = u_{j-2} - u_{j-1}q_j$$
$$v_j = v_{j-2} - v_{j-1}q_j$$

Las siguientes ecuaciones son válidas para todos los renglones j.

$$r_j = au_j + bv_j \quad (1)$$
$$(-1)^j a = r_{j-1}v_j - r_jv_{j-1} \quad (2)$$
$$(-1)^{j-1}b = r_{j-1}u_j - r_ju_{j-1} \quad (3)$$

Teorema 125. *Supongamos que $a = z^{2t}$ y $b = S$ para algún polinomio síndrome S. En el cálculo de el algoritmo Euclideano extendido de a y b, sea j el primer renglón para el cual $\deg(r_j) < t$. Definamos $R_0 = r_j$, $U_0 = u_j$, y $V_0 = v_j$. Entonces R_0, U_0, y V_0 satisfacen las condiciones de el teorema anterior.*

Demostración. Se sigue de el algoritmo Euclideano que $r_j = u_j z^{2t} + v_j S$. Entonces, $R_0 = U_0 z^{2t} + V_0 S$. Además, como $R_0 = r_j$ y $\deg(r_j) < t$, sabemos que $\deg(R_0) < t$. Cómo

$$\deg(v_{j-1}) < \deg(v_j) = \deg(V_0) \text{ and } \deg(r_{j-1}) < \deg(r_j) = \deg(R_0),$$

se obtiene que

$$\deg(v_{j-1}R_0) < \deg(V_0 r_{j-1}).$$

Pero de el algoritmo Euclideano

$$R_0 v_{j-1} - r_{j-1}V_0 = a = z^{2t}.$$

Entonces,

$$\deg(V_0 r_{j-1}) \leq 2t,$$

y como $\deg(r_{j-1}) \geq t$, se sigue que $\deg(V_0) \leq t$. Además

$$\deg(u_{j-1}) < \deg(u_j) = \deg(U_0)\,,$$

implica que

$$\deg(u_{j-1}R_0) < \deg(U_0 r_{j-1}).$$

Por el algoritmo Euclideano

$$R_0 u_{j-1} - r_{j-1}U_0 = b = S.$$

Por lo tanto,

$$\deg(U_0 r_{j-1}) < 2t,$$

y cómo $\deg(r_{j-1}) \geq t$, se sigue que $\deg(U_0) < t$. Sólo falta por demostrar que $(V_0, U_0) = 1$. El algoritmo Euclideano implica que

$$u_{j-1}v_j - u_j v_{j-1} = 1.$$

Entonces,

$$u_{j-1}V_0 - U_0 v_{j-1} = 1,$$

y por lo tanto $(V_0, U_0) = 1$. □

Algoritmo 126 (Algoritmo para Decodificar)**.** *Sea $\mathbb{F}$ un campo con 2^n elementos y sea C un código $RS(2^n - 1, t)$ en $\mathbb{F}[x]$. Supongamos que $c(x) \in C$ es transmitida y que recibimos $r(x) = c(x) + e(x)$ donde $e(x)$ es un polinomio distinto de cero en $\mathbb{F}[x]$ con grado menor que $2^n - 1$.*

1. Cálculese el polinomio síndrome $S(z)$.
2. Construyase la tabla de el algoritmo Euclideano para los polynomios $a(z) = z^{2t}$ y $b(z) = S(z)$ en $\mathbb{F}[z]$, parando al momento que el primer renglon j se satisfaga $\deg(r_j) < t$. Fijemos $R(z) = r_j$ y $V(z) = v_j$.
3. Encuentrese las raíces de $V(z)$. Si $a^{i_1}, a^{i_2}, \ldots, a^{i_k}$ son las raíces de $V(z)$, $r(x)$ tiene errores en las posiciones $x^{-i_1}, x^{-i_2}, \ldots, x^{-i_k}$. Sea e_{-i} el coeficiente de el termino x^{-i} en $e(x)$. Entonces

$$e_{-i} = \frac{R(a^i)}{V\prime(a^i)}.$$

Referencias

[PRE] O. Pretzel, Error-Correcting Codes and Finite Fields, Second Edition, Oxford, New York, 1998.

[KLI] R.E. Klima, N. Sigmon, E. Stitzinger, Applications of Abstract Algebra with MAPLE, CRC Press, Boca Raton, Florida, 2000.

Point Loma Nazarene University
Email address: jjimenez@pointloma.edu