INDICE

§1. INTRODUCCIÓN.

En más de una ocasión debes haber querido enviar un mensaje a un amigo y deseado que ningún intruso se entere del contenido. En alguna otra ocasión, tal vez tú mismo, has sido el intruso que trataba de conocer el contenido de mensajes ajenos, o no tan ajenos. Los seres humanos, a través de la historia, han inventado mecanismos para proteger los mensajes y ponerlos a salvo del ataque de intrusos. Y, como intrusos, también han utilizado el poder de su inteligencia para descifrar mensajes supuestamente bien protegidos. No poco esfuerzo se invierte en esta tarea, pues muchas veces lo que se desea proteger es de gran valor, como la identidad de un ser humano, la seguridad de una transacción comercial o la libertad de un pueblo. La ciencia (o el arte) de proteger información, así como ponerla al descubierto, se llama criptografía y su origen es tan antiguo como la historia misma. Etimológicamente criptografía viene del griego *kryptos* que significa oculto. Otras palabras de igual origen son "críptico" y "cripta". La primera significa "inentendible", la segunda describe el lugar oculto donde se mantienen restos de muertos ilustres.

Tú, el *mensaje,* el *amigo* y el *intruso* definen los cuatro elementos básicos de la criptografía. Esta tiene entonces la doble misión de

i. crear métodos para codificar mensajes y hacerlos crípticos, es decir, protegerlos de los ataques de intrusos y,

ii. crear métodos para quebrar los códigos ajenos, es decir, hacer entendibles los mensajes crípticos.

Hay en la historia universal eventos en los que ambas misiones de la criptografía han jugado roles de trascendental importancia. Durante la segunda guerra mundial los Estados Unidos usaron el lenguaje de los indios navajos, con traductores navajos, para enviar mensajes a los comandos en el frente del Pacífico. Ni japoneses ni alemanes pudieron descifrar la compleja sintaxis del lenguaje. Por otra parte, es conocido el hecho, también de la segunda guerra mundial, de cómo la inteligencia británica, con ayuda del espionaje checoslovaco, fue capaz de descifrar los mensajes codificados del alto comando alemán a la flota del Atlántico, hecho que ayudó a cambiar el destino de la guerra.

La criptografía es una necesidad del mundo moderno. Como actividad sistemática, organizada y de alcance social, su pasado es fuertemente militar o diplomático, sin embargo, con la mecanización de las comunicaciones, la hegemonía de la Internet y la globalización económica y social, la criptografía se ha hecho indispensable en casi toda comunicación.

Basta saber que cuando se hace una transacción comercial en el "mall" local o a través de Internet, la información que contiene la tarjeta de crédito se codifica electrónicamente, a fin de proteger la identidad del cliente y la integridad de la transacción.

Originalmente la criptografía dependía del ingenio y la inspiración de algún especialista y se hacía entonces artesanalmente. La comunicación electrónica de hoy, con su extraordinario volumen y rapidez, ha creado la necesidad de producir métodos científicos para codificar y medir el grado de confiabilidad de los métodos. Con frecuencia la metodología es revisada en la medida en que también se desarrolla metodología para quebrar los códigos. Los métodos son matemáticos y curiosamente muchos de ellos dependen, no de lo que se puede hacer en matemáticas, sino, más bien, de lo que no podemos hacer.

A la segunda misión de la criptografía se le llama *criptoanálisis* y se la distingue de la primera, pues difiere notablemente en propósito y metodología. Quien se dedique a esta profesión, encarará el dilema de ser criptógrafo o criptoanalista, sobre todo porque cuesta determinar cuál de las actividades es más divertida. La realidad es que en ocasiones será una cosa, y en otras la otra. Profesionales en estas disciplinas por lo general son matemáticos o especialistas en computación con grados de maestría o doctoral. Empresas productoras de programado (software), laboratorios de investigación matemática o agencias federales son sus principales fuentes de empleo.

En este módulo usaremos la capacidad de programación de las calculadoras Texas Instruments de la serie TI-84 a TI-86. Cada vez que en el presente módulo requeriramos el uso de la calculadora usaremos la clave "CALC". En el apéndice hay tres programas y una subrutina: POTNS (usa BEZOUT), INVRS y PRIMO, cuyo uso aperecerá en la medida que avancemos en el módulo.

Dentro del los principios del programa CRAIM éste es un *módulo didáctico de matemática para estudiantes o maestros de los niveles primario intermedio y secundario del sistema escolar público* de Puerto Rico. Las ideas fundamentales son generales, ampliamente conocidas y parte del folclor de la comunidad matemática. El autor ha basado la organización del material y asegurado su vigencia en los libros de la bibliografia (pág 36) y recomienda su lectura y consulta a qualquier estudiante o maestro interesado en criptografía.

§2.ARITMETICA MODULAR I

Un caso particular de la aritmética modular es la llamada aritmética del reloj. Cuando a las 10 de la mañana se le agrega 5 horas se llega a las 3 de la tarde, es decir "$10 + 5 = 3$". También si a las 2 de la tarde se le quita 4 horas, el resultado es las 10, lo que equivale a decir que "$2 - 4 = 10$". Esta aritmética del reloj se llama más generalmente *aritmética módulo 12* y se realiza dentro del conjunto $Z_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ cuyos elementos se llaman *enteros módulo 12*. En realidad cualquier número entero es *equivalente* a un entero módulo 12 que se obtiene como el residuo (nunca negativo) de la división entre 12. Por ejemplo "29 es equivalente a 5 módulo 12' y se escribe "$29 \equiv 5(mod 12)$", porque al dividir $29 \div 12$ da (cociente 2 y) residuo 5. Esto también se expresa $mod(29, 12) = 5$, como lo podrás encontrar en tu calculadora (CALC). En efecto, si buscas en el catálogo de funciones encontraras "mod" que cuando lo invoques aparecerá "mod(" y tienes que proveer el *número*, una *coma* y el *módulo.* Queda entonces "mod(29,12)" y al tocar ENTER obtendrás 5. (mirapallá!)

2.1. Adición, substracción y multiplicación: El número 12 es sólo un ejemplo para presentar el concepto de la aritmética módulo N que se realiza en el conjunto $Z_N = \{0, 1, 2, ..., (N-1)\}$, para cualquier entero $N > 1$. A N se le llama "el módulo". Provisto este conjunto de las operaciones de suma, resta y multiplicación se convierte en el *sistema* Z_N. Suma y multiplicación se hacen como aprendimos en la escuela, pero el resultado hay que tomarlo módulo N. Por ejemplo en Z_{13} el producto $8 \times 11 = 10$. (¿correcto?). La resta también, excepto cuando el resultado es negativo. Explica por qué, en Z_{13}, $5 - 10 = 8$.

No te preocupes por lo que signifique *multiplicar horas por horas*, la multiplicación así descrita es puramente formal. De división nos ocuparemos más adelante. Sólo recuerda que estaremos haciendo operaciones en un sistema diferente. Los "números" del sistema en realidad no son números en el sentido corriente. Son elementos de un sistema y sólo nos prestamos los *numerales* 0, 1, 2, 3, ... para entendernos. No hay números negativos, o mejor, todos los números en Z_N son a la vez positivos y negativos. En realidad todo número en este sistema es siempre el negativo de otro. En $a + b = 0$, a es *el negativo* de b y b es *el negativo* de a. Por ejemplo, para efectuar $3 - 8$, en Z_{12}, a 3 le sumamos el negativo de 8 que es 4. Por tanto, $3 - 8 = 3 + (-8) = 3 + 4 = 7$.

Ejercicio 2.1. Haz las operaciones en Z_{12}. Puedes usar función "mod" de la calculadora.

a) 6+6 b) 6×4 c) 4×3 d) $2 - 9$ e) 5^{11} e) 7^{11}

Ejercicio 2.2. Efectúa las siguientes operaciones en el sistema Z_{11}.

a) 6+9 b) 6×2 c) $2 - 9$ d) 4^{10} e) 5^{10}

2.2. División: Tú sabes que si $a \times b = 1$, entonces b es el *recíproco* o *inverso* de a y también a es el inverso de b. Por ejemplo, inverso de $a = 4$ es $b = 0.25$ porque $4 \times 0.25 = 1$. El inverso del entero 4 es el decimal (racional) 0.25. Esta es una anomalía que no queremos en Z_N. Quisiéramos que en Z_N los inversos de los elementos de Z_N caigan en Z_N, como sucede con los negativos. Pero esto no siempre sucede. Por ejemplo en $Z_9 = \{0, ..., 8\}$, ningún elemento es inverso de 3, porque ningún número multiplicado por 3 dará 1. Tendría que dar 10, para que al tomarlo módulo 9, dé 1, y ese entero no existe. Sin embargo $2 \times 5 = 1$. lo que revela que el 5 es el inverso del 2 y, simétricamente, el 2 es el inverso de 5. Podemos afirmar que en Z_9, el 2 es *invertible*, es decir *tiene inverso* y su inverso es $2^{-1} = 5$. Observa la notación: el inverso de a es a^{-1}. Contar con inversos es importante porque nos permiten hacer divisiones y resolver ecuaciones. En efecto, la division $\frac{a}{b}$ la entendemos como $a \times b^{-1}$, es decir multiplicamos a por el inverso del divisor b.

Ecuaciones. Recuerda que una ecuación es una proposición abierta (puede ser cierta o falsa) en la que hay una incógnita (o desconocida) y que clama por ser resuelta. Es decir, debe hallarse el valor o los valores de la incógnita que hagan cierta (satisfagan) la ecuación. Por ejemplo, en los números enteros, la ecuación $2x + 3 = 11$ tiene la solución $x = 4$, porque $2 \times 4 + 3$ es en efecto 11, y, muy importante, 4 es un entero. Es decir esa ecuación la resolvemos dentro de los números enteros.

Las técnicas para resolver ecuaciones en los números regulares, se usan también en Z_N. Sólo se requiere tener cuidado de que las operaciones se hagan en Z_N. Por ejemplo, para resolver $x + 7 = 3$ en Z_{27}, restamos 7 a ambos lados y obtenemos $x + 7 - 7 = 3 - 7$ y de aquí $x = 3 - 7 = -4 = 23 (\text{mod } 27)$. La solución es entonces 23.

Del mismo modo, resolver la ecuación $2x = 7$ en Z_9, resulta fácil. Nos aseguramos que 2 sea invertible. Ahora multiplicamos ambos miembros por el inverso de 2 y obtenemos;

$$(2^{-1}) \cdot 2x = (2^{-1}) \cdot 7$$

de donde

$$5 \cdot 2x = 5 \times 7$$

lo que da

$$x = 8$$

La solución de $2x = 7$, en Z_9, es entonces $x = 8$. Puedes verificar que $2 \times 8 = 7 (\text{mod } 9)$

Elementos invertibles. Elementos de Z_9 que son *invertibles* son 1,2, 4, 5, 7 y 8. (verifícalos.) El resto, 0, 3 y 6 no son invertibles. Lo que es claramente común a estos últimos es que comparten factores con el módulo 9. Todos tienen el factor 3 y 3 es divisor del módulo. Los

invertibles, no comparten factores o divisores con el módulo. Es decir que entre un elemento invertible a y el módulo N el *máximo comun divisor*, *mcd(a,N)*, es 1. Y esa es la condicion *necesaria y suficiente* para que un elemento de Z_N sea invertible. Este hecho se demuestra rigurosamente, no lo haremos aquí, pero le daremos la importancia que tiene.

TEOREMA 1: Un elemento a en Z_N es invertible si y sólo si el $mcd(a, N) = 1$

Ejercicio 2.3. Encuentra todos los elementos invertibles de Z_{27} y parea cada elemento con su inverso.

Ejercicio 2.4. Encuentra todos los elementos invertibles de Z_{11} y parea cada elemento con su inverso.

Ejercicio 2.5. Encuentra todos los elementos invertibles de Z_{24} y parea cada elemento con su inverso.

Ejercicio 2.6. Efectua las divisiones en el sistema que se indica:

1. $1 \div 3$ en Z_{10}
2. $3 \div 8$ en Z_{11}
3. $23 \div 11$ en Z_{27}
4. $(p-2) \div (p-1)$ en Z_p

Ejercicio 2.7. Cuenta los elementos invertibles de Z_p donde p es un número primo.

Ejercicio 2.8. Si p y q son números primos, halla el número de elementos invertibles en Z_{pq}.

Ejercicio 2.9. Resuelve las siguientes ecuaciones lineales en el sistema que se indica

1. $3x = 8$ en Z_{10}
2. $3x = 8$ en Z_{11}
3. $7x + 9 = 8$ en Z_{27}
4. $3x - 7 = 3$ en Z_{10}

Ejercicio 2.10. Si dos elementos $a, b \in Z_N$ son invertibles, ¿es el producto ab invertible en Z_N?. ¿Puedes probarlo?

2.3. Números primos. Se llaman *primos* (no, no son hijos de "titi") porque son primarios. Los primos son los bloques básicos, más elementales de la numeración. Euclides demostró

hace más de 2000 años que existen infinitos primos. Este hecho es parte del interés humano por conocerlos mejor. Sabemos que un número p es primo si no tiene divisores distintos de 1 y p. Esta sencilla propiedad de indivisibilidad, de bloque sólido, es la que permite seguridad en las aplicaciones. Otra propiedad no menos importante es que cualquier otro número es producto único de números primos, es factorizable en primos. La aritmética modular presenta propiedades interesantes cuando el módulo es un número primo. Tres problemas relacionados con primos son de interés en criptografía:

i. Cómo determinar si un número es primo.

ii. Cómo generar números primos.

iii. Cómo hallar la factorización de un número que no es primo.

Estos tres problemas prácticos están íntimamente relacionados y, gracias a la criptografía y a la computación electrónica, han recibido notable atención en el último medio siglo. Existen algoritmos llamados *pruebas de primalidad* que resuelven los tres problemas simultáneamente. Sin embargo no son verdaderas soluciones porque no son lo suficientemente rápidos para lo que se desea. Pero el mejor resultado de las investigaciones es el convencimiento de que los problemas son harto difíciles y se puede confiar que soluciones no aparecerán pronto. A pesar de eso, al computación electrónica ha permitido determinar que ciertos números que se creía primos no lo son y confirmar que otros sí. ¿Te atreverías a afirmar que el número 12345673 es primo?

La prueba de primalidad más sencilla y natural que existe para determinar si un número n es primo, la aprendiste en la escuela. Consiste en dividir n por todos los primos conocidos en orden ascendente hasta hallar uno que dé residuo cero, o hasta tropezar con la raíz cuadrada de n, ¿por qué?. Si sucede lo primero, el número no es primo (compuesto), de lo contrario, el número es primo. Este método se llama prueba de Eratóstenes, por su inventor griego, de hace más de 2000 años.

Ejercicio 2.11. Determina la primalidad de los siguientes números:

a) 91 b) 323 c) 1013 d)2003 e) 12345673

Tecnología al rescate. (CALC) Podemos equipar la calculadora programable con el algoritmo de Eratóstenes. En el apéndice encontrarás el código del programa que se llama PRIMO. Con el poder de esta calculadora puedes manejar números de hasta 10 dígitos —impresionante para los estándares de hace 30 años— pero necesitas algo de paciencia cuando uses números de esa magnitud. Cópialo en tu calculadora y úsalo.

Este programa te dirá si un número es primo; si no lo es te mostrará el primer primo que lo divida. Eso resuelve los problemas i. y iii. El problema ii. se resuelve escogiendo al azar un número q impar del tamaño deseado y aplicándole la prueba PRIMO. Si resulta primo, lo hallaste, si no, trata con $q + 2$ y sigue sumado 2 hasta que lo encuentres. Gauss demostró que los primos están razonablemente bien distribuidos y frecuentes, y calculó su frecuencia. Así, hallar un númer primo *a la medida* ni es difícil ni toma mucho tiempo.

Ejercicio 2.12.(CALC) Determina la primalidad de los siguientes números:

a) 911 b) 323157 c) 7291013 d)2003117 e) 12345673

Ejercicio 2.13. (CALC) Usa el programa PRIMO para hallar todos los factores del número 90019091

Ejercicio 2.14. (CALC) Halla el primer número primo mayor que 1001

Ejercicio 2.15. (CALC) Primos gemelos son primos cuya diferencia es 2, es decir son primos y a la vez impares consecutivos. Halla el primer par de primos gemelos mayores que 10000.

§3. LO QUE ES DEL CESAR

Mucho antes de la computación electrónica moderna, se hacía criptografía con métodos, para nuestra visión contemporánea, francamente primitivos. Los mensajes se codificaban muy sencillamente y eran fácilmente decodificables. En un mundo de poca comunicación, no parecía haber necesidad de métodos demasiados sofisticados. Veremos sólo unos pocos de estos métodos, aquellos que tienen todavía alguna relevancia en la criptografía moderna.

3.1 Nomenclatura. Ahora que entramos en la materia misma de la criptografía, establezcamos el lenguaje conveniente que hemos de usar en adelante; algunos términos son neologismos. Al mensaje o texto original lo llamaremos *texto llano*. *Encriptar* será el proceso de convertir un texto llano en *texto críptico*. Quien envía el mensaje encriptado es el *emisor* , el destinatario es el *receptor*. *Decriptar* consiste de revertir, con el uso de una *clave* , el proceso de encriptar, es decir, recuperar el texto llano y esto lo hace el receptor quien conoce la clave de antemano. *Quebrar* el código consiste en descubrir (por medios alternos) la clave para revelar el mensaje y es por supuesto el divertido trabajo del *criptoanalista.*

3.2. Código del César. Se dice que en la antigua Roma, Julio César enviaba mensajes encriptados a sus generales en el frente. Para ello, cada letra del mensaje era reemplazada por la letra ubicada tres letras más adelante en el alfabeto. Así el texto llano "ATAQUEN", se convierte en texto críptico "DWDTXHQ". Puedes cotejar que a la letra A le corresponde la letra D que está tres letras más adelante en el alfabeto, después de B y C; y así con las otras letras. Modernamente usaremos el alfabeto español de 27 letras o *caracteres* que ocupan un solo espacio . Las letras "CH" y "LL" cuentan cada una como dos caracteres independientes.

A fin de manejar más sistemáticamente este código y otros, establecemos la correspondencia "natural" uno-a-uno entre las 27 letras del alfabeto y los 27 elementos de Z_{27}. Llamaremos a esto la *Tabla de Equivalencia Numérica* (TEN).

A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	2	3	4	5	6	7	8	9	10	11	12	13	14
Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	
15	16	17	18	19	20	21	22	23	24	25	26	0	

Para encriptar un mensaje, entonces, se identifica cada letra con su número correspondiente 'x' que luego se le transforma en $x + 3 (\text{mod } 27)$ y a ese nuevo número se le devuelve a la letra que le corresponde.

Ejemplo 3.1. Encriptemos "MAYO":

$$\text{MAYO} \longrightarrow 13.1.26.16. \xrightarrow{x+3(\text{ mod } 27)} 16.4.2.19 \longrightarrow \text{ODBR}$$

Y "ODBR" es el texto críptico que el emisor transmite. El receptor *conoce la clave* que consiste simplemente en aplicar el proceso inverso, es decir restar 3 unidades en Z_{27} lo que equivale a sumar $24(\text{mod } 27)$. Ahora decriptemos "ODBR"

$$\text{ODBR} \longrightarrow 16.4.2.19 \xrightarrow{x+24(\text{ mod } 27)} 13.1.26.16. \longrightarrow \text{MAYO}$$

Función de encriptar. Convertir los caracteres en números permite usar el poder de las matemáticas en el proceso. Tanto $x + 3(\text{mod } 27)$ como $x + 24(\text{mod } 27)$ son *funciones*. Las funciones son reglas que dicen cómo se transforman elementos de un *dominio* en elementos de un *rango*. Ese dominio son los objetos matemáticos "enteros módulo 27", Z_{27}. Podemos representarlas con la notación funcional

$$f(x) = x + 3(\text{mod } 27) \qquad \text{y} \qquad g(x) = x + 24(\text{mod } 27)$$

Y es más, $g(x)$ es *función inversa* de $f(x)$. Esto quiere decir que la función g *deshace* lo que f *hace* y —simétricamente— f deshace lo que g hace. Dicho de otro modo, si ponemos a actuar una función detrás de la otra sobre un objeto $x \in Z_{27}$, hallaremos que nada le habrá pasado a x, es decir, la segunda función restaura x que es precisamente lo deseado en criptografía:

$$g(f(x)) = x(\text{mod } 27) \qquad \text{y} \qquad fg(x) = x(\text{mod } 27)$$

Desglosada la primera ecuación en aritmética módulo 27, se ve como:

$$g(f(x)) = g(x + 3) = (x + 3) + 24 = x + (3 + 24) = x + 27 = x$$

Ejercicio 3.1. En Z_{27}, halla la inversa $g(x)$ de la función $f(x) = x + 9$ y verifica que en efecto f y g son mutuamente inversas.

Clave privada. Para decriptar, el receptor debe conocer la clave —que es la función inversa— que en este caso es $x+24(\text{ mod } 27)$. La posibilidad de comunicación criptográfica depende de que emisor y receptor estén de acuerdo en el sistema que han de usar y en la clave a ser usada. Si el emisor usa 5 en lugar de 3, el receptor debe estar informado para usar 22 en lugar de 24. Este detalle obliga a que antes de usar un sistema criptográfico, emisor y receptor deben

haberse comunicado no criptográficamente. Pudiera ser una entrevista, como posiblemente tuvo que hacer el César con sus generales y éstos debieron recordar la clave y no revelarla. Este sistema en que emisor y receptor se entrevistan y se comunican la clave se llama y de *clave privada*, y es simétrico, es decir los roles de emisor y receptor pueden intercambiarse. Más adelante veremos otros sistemas que son de clave pública, no simétricos pero tan seguros como los mejores.

Criptoanálisis. Quebrar el código del César es un trabajo muy sencillo, aunque un mensaje muy corto sería difícil de descifrar. Un mensaje largo en cambio hace la clave más vulnerable. Un criptoanalista hará un análisis para detectar la letra más frecuente en el mensaje y la pareará con la letra más frecuente en texto en español. Basta ese pareo y la clave queda revelada.

En texto ordinario de español las letras más frecuentes y sus porcentajes aproximados son como sigue:

LETRA	PORCENTAJE
E	14.6 %
A	10.8 %
S	9.2 %
O	8.6 %
R	7.2 %
I,N,T	5.6

Debido a la fuerte preponderancia de la letra "E", cualquier criptoanalista decidirá de primera instancia que la letra más frecuente en el texto críptico interceptado ha de corresponder precisamente a "E" y eso quebrará el código.

Ejercicio 3.2. Por medios "impropios" se ha interceptdo el siguiente mensaje. Se sabe que fue encriptado con el método del César pero con una clave diferente. Descifra el mensaje

ALCONOBEOGLLVVZGOCOVNSOVZDOODELXFMVLXÑZ

3.3. César mejorado. Un simple desplazamiento de letras es un sistema cuya clave es muy fácil de detectar. El sistema del César puede ser ligeramente mejorado con la introducción de un nuevo parámetro en la función de encriptar y convertirla de un simple desplazamiento en una *función afín*. Este nuevo sistema no es demasiado superior al del César, pero la función tiene atributos útiles para lo que viene. Notarás que hay sólo 26 posibles desplazamientos tipo César. Mejorando César aumentaremos notablemente el número de funciones de encriptar

Con el fin de señalar con claridad el *dominio* y el *rango* de una función usaremos la

notación funcional explícita siguiente

$$f : Z_n \longrightarrow Z_m$$

la cual dice que f toma valores en Z_n (su dominio) y los transforma en valores de Z_m (su rango). Una función queda definida por una regla que dice qué le corresponde cada elemento del dominio. Las funciones afines que usaremos para mejorar el César tienen como las anteriores dominio y rango iguales a Z_{27} y están definidas por dos parámetros a y b:

$$f(x) = ax + b \pmod{27}$$

donde a y b son elementos de Z_{27}, b puede ser cualquiera, pero a debe ser invertible.

La propiedad básica de toda función de encriptar es que sea uno-a-uno (1-1). Esto significa que no debe haber dos letras distintas que se conviertan en la misma. Las translaciones de César tienen claramente esa propiedad. Sin embargo, la función $f(x) = x^2$ en Z_{27}, por ejemplo, sería muy mala función de encriptar porque $f(6) = 6^2 = 9 (\text{mod } 27)$ y $f(21) = 21^2 = 9 (\text{mod } 27)$. Entonces las letras "F" y "T" se encriptarían ambas como "I", creando ambigüedad indeseada .

Que a sea invertible nos asegura que la función afín $f(x) = ax + b (\text{mod } 27)$ sea 1-1. En efecto, si

$$ax + b = ay + b$$

restando b a ambos lados obtenemos

$$ax = ay$$

Como a es invertible multiplicamos ambos miembros por el inverso a^{-1} (igual que dividir) y obtenemos

$$a^{-1} \cdot ax = a^{-1} \cdot ay$$

que se reduce a

$$x = y$$

lo cual quiere decir que *caracteres que se encriptan en caracteres iguales deben ser iguales.*

Otro consecuencia vital del hecho que a sea invertible en Z_{27} es que, como en el caso de César, de la función de encriptar, $f(x) = ax + b$, se obtiene la función de decriptar. Piensa que si se transforma x, "multiplicando por a y luego sumando b", desharemos este proceso "restando b y luego dividiendo por a", y en ese orden. Otra forma de ver esta deducción es resolviendo la ecuación $ax + b = z$, para ver cómo se obtiene x a partir de z. En efecto,

$$ax + b = z$$

$$ax = z - b$$
$$x = a^{-1} \cdot (z - b) = \frac{z - b}{a}$$

y se ve claramente la necesidad de dividir por a.

Criptoanálisis. A fin de quebrar el código de César mejorado, también se recurre a la tabla de frecuencias; pero al haber dos parámetros, será necesario contar con doble información. Por ejemplo, si supiéramos que la letra "E" se convirtió en "Q" y la "A" en "M", numéricamente tendríamos $5 \mapsto 18$ y $1 \mapsto 13$, por lo que para conocer los parámetros a y b debemos resolver las ecuaciones: $\{f(5) = 18 \quad \text{y} \quad f(1) = 13\}$, es decir,

$$\begin{cases} 5a + b & = 18 \\ 1a + b & = 13 \end{cases} \tag{6}$$

Si restamos verticalmente para eliminar b obtenemos:

$$4a = 5$$

de donde

$$a = \frac{5}{4} = 5 \times 4^{-1} = 5 \times 7 = 8 \pmod{27}$$

$a = 8$ no tiene factores en común con 27, lo que hace que a sea invertible.

Con $a = 8$, se puede conseguir b con sólo substituir en la segunda ecuación $1a + b = 13$ y se obtiene $8 + b = 13$, de donde $b = 13 - 8$ ó $b = 5$. Entonces la función para descifrar el mensaje es

$$g(x) = \frac{x - 5}{8} = 17x + 23 \quad \text{por} \quad \text{que?}$$

Ejercicio 3.3 Explique por qué $\dfrac{x - 5}{8} = 17x + 23$

Ejercicio 3.4. Por medios "impropios" se ha interceptdo el siguiente mensaje. Se sabe que fue encriptado con el método del César mejorado y se sospecha que al texto llano "SOL" le corresponde el texto encriptado "ELR". Descifra el mensaje

RQ KEKBADQ FK RQ WQJKWQJZAQ KE EÑ RZVKZJQF AQBJLZ

Ejercicio 3.5 Investiga cuántas funciones afines existen con parámetros a y b en Z_{27} (Cuidado, la respuesta no es 702.)

§4. ARITMETICA MODULAR II: INVERSOS

4.1. Cálculo de inversos. El ejercicio 3.3 se puede completar si se halla el inverso de $8(\text{mod } 27)$. Hasta ahora hemos calculado inversos por proceso exhaustivo, recorriendo la lista de los enteros módulo 27. Por ejemplo, para hallar el inverso de 8 hacemos los productos 8×2, 8×3, ..., hasta obtener uno de esos productos igual a $1(\text{mod}27)$, después de 16 pasos. En efecto $8 \times 17 = 136 \equiv 1(\text{mod}27)$. Concluímos que 17 es el inverso de 8 en Z_{27} y podemos escribir $17 = 8^{-1}(\text{mod}27)$, el inverso de 8. Este método funciona bien si el módulo es relativamente pequeño. Mejores métodos serán necesarios para módulos más grandes.

4.2. **Máximo Común Divisor (*mcd*)**. Recordarás que el máximo común divisor de dos números a y b es el divisor común más grande de los dos números. Por ejemplo, para $a = 30$ y $b = 18$, 3 es un divisor común pero no es el máximo. Sabemos que el máximo es 6. Para denotar eso escribimos

$$mcd(30, 18) = 6.$$

Ahora, como 6 es divisor común de 30 y 18, también lo es de cualquier múltiplo de 30 y de cualquier múltiplo de 18, es decir 6 divide a $30x$ donde x es cualquier número entero, positivo o negativo. También divide a cualquier múltiplo de 18, $18y$, sea y positivo o negativo. Es más, si 6 aparece como divisor de $30x$ y $18y$, también será divisor de la suma $30x + 18y$, a la que llamamos una *combinación lineal* (o simplemente *combinación*) de 30 y 18. Entonces creamos el conjunto C de todas las combinaciones de 30 y 18

$$C = \{30x + 18y : x, y \quad \text{números} \quad \text{enteros}\}.$$

Por ejemplo, $30 \times 2 + 18 \times 3 = 114 \in C$ y también $30 \times (-5) + 18 \times 7 = -24 \in C$. Observarás que C puede contener números positivos y negativos y que siempre 6 es divisor de esos números. Ahora contesta esta pregunta. ¿A qué crees que es igual la combinación positiva más pequeña de C?

Acertaste, es 6. No puede ser 1, ni 2, ..., ni 5, porque a esos nńeros 6 no los divide. Eso quiere decir que 6 es una combinación de 30 y 18. En efecto, $6 = 30 \times (-4) + 18 \times 7$. La trascendencia de esto es que el máximo común divisor de a y b siempre es combinación de a y b, es decir hay números enteros m y n tales que

$$mcd(a, b) = am + bn$$

y este hecho se conoce como el Teorema de Bezout. Se le demuestra con mucho rigor y aquí le damos la importancia que merece:

BEZOUT: Si a y b son enteros > 0, existen enteros m y n tales que $mcd(a, b) = am + bn$

Ejercicio 4.1, Expresa como combinacion el máximo común divisor de los pares de enteros en cada caso.

a) 15 y 9 b) 6 y 14 c) 8 y 27 d) 224 y 98

Cuando el *mcd* es 1, el teorema de Bezout tiene importantes consecuencias. Por ejemplo, ya sabemos que $mcd(2,9) = 1$ y que 5 es el inverso de 2 en Z_9 (ver ejemplo). Entonces por Bezout hay una combinación $2 \times 5 + 9 \times (-1) = 1$ que en Z_9 podemos escribirla como

$$2 \times 5 + 9 \times 8 = 1,$$

pues $-1 \equiv 8 \bmod 9$. Si miramos el lado izquierdo de esta expresión dentro de Z_9,

$$9 \times 8 \equiv 0 (\bmod\ 9)$$

lo que nos deja

$$2 \times 5 = 1 (\bmod\ 9),$$

es decir, 5 es el inverso de 2 en Z_9.

Ejercicio 4.2., Halla, en el módulo indicado, los inversos de los números siguientes.

a) 7 en Z_9 b) 20 en Z_{27} c) 8 en Z_{13} d) 10 en Z_{81}

División larga. Vamos en busca del método para calcular inversos y para ello usaremos los residuos de la división de enteros. Cuando dividimos a entre b obtenemos un cociente q y un residuo r

$$b \overset{q}{\overline{\big|\, a}}$$
$$\qquad\quad r$$

o mejor, $a = b \times q + r$, donde $0 \leq r < q$ (el residuo debe ser menor que el divisor) . Si despejamos r tenemos

$$r = a + b \times (-q)$$

lo que muestra a r como una combinación de a y b, pero no es el *mcd*, todavía. Por ahora r comparte los divisores de a y b. Tenemos la esperanza de que si ahora dividimos el cociente entre el residuo obtendremos un nuevo residuo menor que el anterior y eventualmente llegaremos al *mcd*. Veamos el siguiente ejemplo:

Ejemplo 4.1. Hallemos el inverso de 10 módulo 27 y en el camino aprendamos el *algoritmo.* (Un algoritmo es un secuencia de pasos conducentes a un resultado.) Empecemos por dividir $27 \div 10$ y obtener el residuo, y repetir el proceso:

$$27 \div \mathbf{10} \implies 27 = 10 \times 2 + 7 \implies \mathbf{7} = 27 + 10 \times (-2) \tag{1}$$

$$10 \div \mathbf{7} \implies 10 = 7 \times 1 + 3 \implies \mathbf{3} = 10 + 7 \times (-1) \tag{2}$$

$$7 \div \mathbf{3} \implies 7 = 3 \times 2 + 1 \implies \mathbf{1} = 7 + 3 \times (-2) \tag{3}$$

Como el último residuo es 1, las ecuaciones (1), (2) y (3) son todas combinaciones de residuos y cocientes. Ahora hacemos sustituciones algebraicas (no operaciones) en ascenso para escribir 1 como combinación de 10 y 27. En efecto, el 3 de (2) va a (3):

$$1 = 7 + 3 \times (-2) = 7 + \underbrace{[10 + 7 \times (-1)]}_{=3} \times (-2) = 10 \times (-2) + 7 \times 3$$

y ahora el tomamos el 7 de (1):

$$1 = 10 \times (-2) + \underbrace{[27 + 10 \times (-2)]}_{=7} \times 3 = 27 \times 3 + 10 \times (-8)$$

y al tomar todo en Z_{27} tenemos

$$1 = 10 \times 19.$$

Es decir, 19 es el inverso de 10 en Z_{27}.

Ejercicio 4.3. Usa el algortitmo del ejemplo 4.2 para hallar los inversos según se indica:

a) de 13 en Z_{27} b) de 19 en Z_{50} c) de 9 en Z_{100} d) de 32 en Z_{81}

Tecnologia al rescate. (CALC) Este algoritmo (algo tedioso) se puede codificar en cualquier calculadora programable. Coteja el apéndice donde aparece el código para las calculadoras TI. Programa tu calculadora con esas dos unidades de código: el programa INVRS y el módulo BZOUT. Se ejecuta el programa, no el módulo. BZOUT es sólo una subrutina auxiliar del programa y calcula los enteros m y n del teorema. El programa INVRS recibe un número n y un módulo M y cuando $gcd(n, M) = 1$, devuelve el inverso de n en Z_M. Con ello puedes calcular cualquier inverso. Los vamos a necesitar en lo que viene.

Ejercicio 4.4. (CALC) Usa el programa INVRS para hallar inversos según se indica:

a) de 47 en Z_{100} b) de 129 en Z_{1000} c) de 81 en Z_{512} d) de 512 en Z_{8113}

Ejercicio 4.5. (CALC). Toma $N = 1000$ y halla dos elementos a y b invertibles en Z_{1000} y también halla sus inversos a^{-1} y b^{-1}. Halla el producto ab. Haz lo siguiente::

1. Verifica que ab es invertible y halla el inverso de ab.
2. Halla el producto de los inversos a^{-1} y b^{-1}
3. Verifica que el inverso de ab hallado en 1. es congruente, módulo 1000, con el producto de inversos de 2.
4. Explica tus propias conclusiones obtenidas por 3.

§5. MATRICES Y DIGRAFÍAS

El análsis de frecuencias con letras tan prominentes como "E" y "A" facilita notablemente el criptoanálisis, lo cual no es deseable para el critptógrafo. Una forma de paliar esta debilidad es usar pares de letras o *digrafías* (doble grafía) como unidades básicas del mensaje. En "HOLA" reconocemos las digrafías "HO" y "LA". Si aún mantenemos la correspondencia A→ 1, B→ 2,..., Z→ 0, de caracteres con elementos de Z_{27}, de la tabla TEN (Pág 8) a cada digrafía le hacemos corresponder el par ordenado de números formado por los correspondientes a cada letra. A "HO" le corresponde el par ordenado $(8, 16)$, que lo tratamos como *vector* y entonces usamos matrices para encriptarlo.

Una *matriz* 2×2 (dos por dos) es un arreglo de cuatro (4) números escritos en dos filas y dos columnas, en la forma

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Este arreglo sirve para transformar pares de números, llamados *vectores*, (x, y) en otros vectores en la siguiente forma:

$$(x, y) \xrightarrow{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} (ax + by, cx + dy)$$

lo cual, como ves en la siguiente línea, es una *multiplicación* de la matriz por el vector. La aritmética debe ser modular, por supuesto.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix} \tag{1}$$

Por ejemplo, $\begin{pmatrix} 3 & -4 \\ 5 & 1 \end{pmatrix} \cdot \begin{pmatrix} 8 \\ 16 \end{pmatrix} = \begin{pmatrix} 3 \times 8 + (-4) \times 16 \\ 5 \times 8 + 1 \times 16 \end{pmatrix} = \begin{pmatrix} -40 \\ 56 \end{pmatrix}$

Esta doble encriptación de una digrafía, 'AB' por ejemplo, evita que una letra sea fácilmente reconocida por la frecuencia de su aparición. De todos modos, es posible hacer una tabla de frecuencias de digrafías (véase ejercicio 5.1) y utilizarla para decriptar, pero usaremos un mecanismo algo diferente y veremos el poder de las matrices. Antes veamos, mediante un ejemplo, cuándo una matriz permite definir una función que sea útil en criptografía, es decir, que sea uno-a-uno y que, conociendo la clave, permita decriptar con facilidad.

Ejemplo 5.1. Usaremos una función de encriptar definida por la matriz $\begin{pmatrix} 3 & 7 \\ 2 & 5 \end{pmatrix}$ y encriptaremos el mensaje "TODO". En este mensaje de 4 letras hay dos digrafías "TO" y

"DO" que transformadas a su equivalente numérico en Z_{27} (tabla TEN), dan los vectores $(21, 16)$ y $(4, 16)$. A la función la llamamos f y su acción se expresa

$$TO \to f\begin{pmatrix}21\\16\end{pmatrix} = \begin{pmatrix}3 & 7\\2 & 5\end{pmatrix}\begin{pmatrix}21\\16\end{pmatrix} = \begin{pmatrix}3\times 21+7\times 16(\text{mod}27)\\2\times 21+5\times 16(\text{mod}27)\end{pmatrix} = \begin{pmatrix}13\\14\end{pmatrix} \to MN$$

$$DO \to f\begin{pmatrix}4\\16\end{pmatrix} = \begin{pmatrix}3 & 7\\2 & 5\end{pmatrix}\begin{pmatrix}4\\16\end{pmatrix} = \begin{pmatrix}16\\7\end{pmatrix} \to OG$$

Así "TODO" se transforma en "MNOG". Observa que el texto críptico oculta bien la repetición de letras del texto llano. La razón es que las unidades de encriptación son las digrafías y no los caracteres aislados. Si el número de caracteres en el texto llano no fuera par, el agregado de un carácter innocuo permitirá encriptar con facilidad. El mensaje ATAQUEN puede se transmitido como ATAQUENN.

Quedan las preguntas básicas de si esta función es buena para encriptar, es decir, si digrafías diferentes se encriptan en digrafías diferentes y si, conocida la clave, es posible decriptar con facilidad. Contestemos la segunda pregunta primero; la respuesta de la primera seguirá como conscuencia.

Usemos la matriz anterior. Una digrafía representada por el vector (x, y) se encripta en el vector (u, v), por acción de la matriz:

$$\begin{pmatrix}3 & 7\\2 & 5\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}3x+7y\\2x+5y\end{pmatrix} = \begin{pmatrix}u\\v\end{pmatrix}$$

lo que nos da un sistema de ecuaciones lineales

$$\begin{cases} 3x+7y &= u\\ 2x+5y &= v\end{cases} \tag{2}$$

y ahora decriptar consiste en, conocido el vector (u, v), encontrar el vector (x, y). Usaremos el método que sigue.

5.1 Método de eliminación. Si nunca viste este método, ahora es el momento de aprenderlo. Para eliminar temporalmente la variable 'y' multiplicamos (mod27) estratégicamente las ecuaciones de (2); por 5 la primera, y por -7 la segunda y obtenemos el sistema equivalente:

$$\begin{cases} 5\times(3x+7y) &= 5u\\ -7\times(2x+5y) &= -7v\end{cases} \longrightarrow \begin{cases} 15x+35y &= 5u\\ -14x-35y &= -7v\end{cases}$$

Al hacer la suma verticalmente, hemos eliminado la variable 'y' y obtenemos 'x':

$$x = 5u-7v \quad = \quad 5u+20v(\text{mod}27) \tag{3}$$

Ahora podemos elegir eliminar la variable 'x' para obtener 'y'; pero es más fácil reemplazar la fórmula de $x = 5u - 7v$, en una de las ecuaciones originales de (2)—la primera por ejemplo— $3x + 7y = u$, y obtener:

$$3(5u - 7v) + 7y = u$$

y luego despejar 'y'

$$15u - 21v + 7y = u \qquad \longrightarrow \qquad 7y = -14u + 21v$$

de donde

$$y = \frac{-14u + 21v}{7} \quad = \quad \frac{-14}{7}u + \frac{21}{7}v \quad = \quad -2u + 3v,$$

es decir,

$$y = 25u + 3v(\text{mod}27) \tag{4}$$

Las ecuaciones (2) y (3) juntas muestran cómo el vector (u, v) se transforma (regresa al) vector (x, y). Así

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 5u + 20v \\ 25u + 3v \end{pmatrix} = \begin{pmatrix} 5 & 20 \\ 25 & 3 \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}$$

Como recordarás de allá arriba, el texto llano "TODO", por uso de la matriz $\begin{pmatrix} 3 & 7 \\ 2 & 5 \end{pmatrix}$, se encriptaba como "MNOG". Verifiquemos ahora que en efecto podemos decriptar el texto críptico "MNOG". Lo descomponemos en digrafías y hallamos sus respectivos vectores: "MN"→ (13,14) y "OG"→ (16,7) y les aplicamos la matriz $\begin{pmatrix} 5 & 20 \\ 25 & 3 \end{pmatrix}$, la cual define una nueva función g:

$$MN \to g \begin{pmatrix} 13 \\ 14 \end{pmatrix} = \begin{pmatrix} 5 & 20 \\ 25 & 3 \end{pmatrix} \begin{pmatrix} 13 \\ 14 \end{pmatrix} = \begin{pmatrix} 5 \times 13 + 20 \times 14(\text{mod}27) \\ 25 \times 13 + 3 \times 14(\text{mod}27) \end{pmatrix} = \begin{pmatrix} 21 \\ 16 \end{pmatrix} \to TO$$

y también

$$OG \to g \begin{pmatrix} 16 \\ 7 \end{pmatrix} = \begin{pmatrix} 5 & 20 \\ 25 & 3 \end{pmatrix} \begin{pmatrix} 16 \\ 7 \end{pmatrix} = \begin{pmatrix} 5 \times 16 + 20 \times 7(\text{mod}27) \\ 25 \times 16 + 3 \times 7(\text{mod}27) \end{pmatrix} = \begin{pmatrix} 4 \\ 16 \end{pmatrix} \to DO$$

Claramente *g deshace lo que f hace*, es decir g es la función inversa de f.

Ejercicio 5.1. Haz una tabla de frecuencias de digrafías. Toma un texto español genérico de no más de 500 palabras y divídelo en digrafías. Haz una tabulación y determina empíricamente cuáles son las digrafías más frecuentes.

5.2. Matriz inversa. La última afirmación respecto de f y g es posible ponerla en términos de matrices de la siguiente forma:

$$\text{La matriz} \qquad B = \begin{pmatrix} 5 & 20 \\ 25 & 3 \end{pmatrix} \quad \text{es inversa de la matriz} \quad A = \begin{pmatrix} 3 & 7 \\ 2 & 5 \end{pmatrix}$$

Pero esta es una relación simétrica, por lo que podemos escribir:

$$\begin{pmatrix} 5 & 20 \\ 25 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 3 & 7 \\ 2 & 5 \end{pmatrix} \qquad \text{y} \qquad \begin{pmatrix} 3 & 7 \\ 2 & 5 \end{pmatrix}^{-1} = \begin{pmatrix} 5 & 20 \\ 25 & 3 \end{pmatrix}$$

Podemos verificar que una matriz es inversa de otra si la una *deshace lo que la otra hace*, pero eso no es lo más práctico. Recordemos que en Z_{27}, 7 es inverso de 4 porque $4 \times 7 = 1$, la *identidad multiplicativa* de Z_{27}; aquel elemento innocuo, el que no multiplica a nadie. Para las matrices entonces necesitamos dos conceptos: el de *multiplicación* y el de *identidad multiplicativa*. Se multiplican dos matrices como una extensión de la forma de multiplicar una matriz por un vector, ya usada en (1), del modo que sigue:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x & s \\ y & t \end{pmatrix} = \begin{pmatrix} ax + by & as + bt \\ cx + dy & cs + dt \end{pmatrix} \tag{5}$$

Con esta fórmula veremos que la matriz identidad es $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$; y ante la multiplicación es innocua. En efecto:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Ahora podemos verificar que A y B son inversas mutuas, es decir, $A \cdot B = B \cdot A = I$

$$A \cdot B = \begin{pmatrix} 3 & 7 \\ 2 & 5 \end{pmatrix} \cdot \begin{pmatrix} 5 & 20 \\ 25 & 26 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Así como no todo elemento de Z_N es invertible, también no toda matriz es invertible. Podemos tratar de "descubrir" una condición para que una matriz 2×2 sea invertible. Repitamos algebraicamente el proceso que nos llevó a encontrar el vector (x, y) a partir de (u, v). Comenzamos con el sistema de ecuaciones (2)

$$\begin{cases} ax + by &= u \\ cx + dy &= v \end{cases} \tag{6}$$

y con el método usado eliminamos 'y'. Para ello multiplicamos estratégicamente por d y $-b$

$$\begin{cases} d \times (ax+by) & = du \\ -b \times (cx+dy) & = -bv \end{cases} \longrightarrow \begin{cases} adx+bdy & = du \\ -bcx-bdy & = -bv \end{cases}$$

Sumar verticalmente elimina los términos con y y nos queda

$$adx - bcx = du - bv, \quad \text{o} \quad \text{mejor}, \quad (ad-bc)x = du - bv \tag{7}$$

Ahora, despejar 'x' depende de que podamos dividir por ese factor $ad-bc$. Es decir, ese factor $(ad-bc)$, llamado el *determinante (det)* de la matriz $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, debe ser invertible como elemento de Z_N. Este hecho es importante y por eso lo enmarcamos:

La matriz $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ es invertible si y sólo si $\quad det(A) = ad - bc \quad$ es invertible en Z_N

Ejemplo 5.2. Con toda esta nueva información se hace muy fácil encontrar mecanismos para encriptar mensajes. Todo lo que necesitamos es una matriz invertible. Lanzamos al azar cuatro números modulo 27: $5, 2, 9, 21$ que organizamos en una matriz $K = \begin{pmatrix} 5 & 2 \\ 9 & 21 \end{pmatrix}$. Calculamos su determinante: $det(K) = 5 \times 21 - 2 \times 9 = 6 (\operatorname{mod} 27)$. Pero no nos sirve porque 6 no es invertible en Z_{27}. Debemos escoger con más cuidado:

$$M = \begin{pmatrix} 5 & 2 \\ 9 & 1 \end{pmatrix}$$

Su determinante es $det(M) = 5 \times 1 - 9 \times 2 = -13 = 14 (\operatorname{mod} 27)$ y como $mcd(14, 27) = 1$, el determinante es invertible y por tanto M es buena para encriptar digrafías. Para decriptar necesitamos la matriz inversa de M, pero eso lo resolverás en un ejercicio.

Ejercicio 5.3. En Z_{27} encuentra las matrices inversas. Verifica por multiplicación. Debes obtener la matriz identidad I

a) $A = \begin{pmatrix} 5 & 3 \\ 8 & 5 \end{pmatrix}$ b) $B = \begin{pmatrix} 9 & 7 \\ 5 & 4 \end{pmatrix}$ c) $C = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ d) $M = \begin{pmatrix} 5 & 2 \\ 9 & 1 \end{pmatrix}$

5.2. Cálculo de la matriz inversa. Retomemos la fórmula de (7)

$$(ad-bc)x = du - bv \tag{8}$$

y llamemos D al determinante de esa matriz genérica $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

$$D = det(A) = ad - bc$$

Entonces la ecuación anterior (7) se escribe

$$D \cdot x = du - bv$$

Suponiendo que D es invertible en Z_N, estamos autorizados a dividir, entonces

$$x = \frac{d}{D}u + \frac{-b}{D}v \tag{9}$$

Y ahora te invito (te urjo) a que tomes el sistema (6), y lo que hicimos para la variable 'x', lo repitas paso a paso para la variable 'y'. Hallarás el mismo determinante y podrás despejar 'y' como sigue:

$$y = \frac{-c}{D}u + \frac{a}{D}v \tag{10}$$

Entonces la matriz que retorna (u, v), a (x, y) es

$$\begin{pmatrix} \frac{d}{D} & \frac{-b}{D} \\ \frac{-c}{D} & \frac{a}{D} \end{pmatrix} \quad \text{o, mejor,} \quad \begin{pmatrix} dD^{-1} & -bD^{-1} \\ -cD^{-1} & aD^{-1} \end{pmatrix}$$

Y esta es la matriz inversa de $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$

Fácil recordarlo: "Vira la diagonal principal, niega la secundaria y todo lo cortas por D"

Ejercicio 5.3. Halla las inversas de las matrices siguientes en el sistema que se indica. No dejes denominadores

a) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ en Z_9

b) $\begin{pmatrix} 7 & 4 \\ 4 & 3 \end{pmatrix}$ en Z_{12}

c) $\begin{pmatrix} 4 & 0 \\ 0 & 7 \end{pmatrix}$ en Z_{27}

d) $\begin{pmatrix} 6 & 1 \\ 2 & 5 \end{pmatrix}$ en Z_{27}

Ejercicio 5.4. Demuestra que si multiplicas dos matrices invertibles, el resultado es también una matriz invertible.

§6. SUPERPOTENCIAS

6.1. Petit Fermat. Las potencias son interesantes en estos sistemas *finitos* (lo contrario de infinito). Ya en los Ejercicios 2.1 y 2.2 has tenido la oportunidad de calcular varias potencias, especialmente 4^{10} y 5^{10} en Z_{11}. En ambos casos habrás obtenido 1. (¿no?, revisa tus cálculos). Para hacer criptografía de clave pública necesitaremos hacer cálculos de potencias con exponentes muy grandes. Les llamaré superpotencias.

Como podrás intuir, cuando calculamos potencias grandes de $a \in Z_N$, multiplicamos a por sí mismo repetidas veces. Entonces empezamos a recorrer los elementos de Z_N y eventualmente reencontraremos al mismísimo elemento a. Es decir, existe un exponente e tal que $a^e = a$. Piensa en lo que pasó en el pasito anterior: tuvimos $a^{e-1} = 1$ (¿verdad?).

En *Teoría de Números* se demuestra lo que ya has verificado en los Ejecicios 2.2, que cuando el módulo es un número primo p, toda potencia de exponente $p-1$, (salvo 0) siempre da 1 (mod p). Verifiquémoslo en un caso muy sencillo. Por ejemplo si $p = 5$, primo, $p - 1 = 4$ entonces $2^4 = 16 \equiv 1(\text{mod } 5)$, $3^4 = 81 \equiv 1(\text{mod } 5)$ y $4^4 = 256 \equiv 1(\text{mod } 5)$. Tú puedes verificarlo con otros números usando la calculadora (CALC). Escoge el primo p, toma un número a menor que p y calcula a^{p-1}. Te dará un número muy grande. Si te da en notación científica, le estás exigiendo demasiado a tu calculadora, haz un cálculo más modesto. Usa la función "mod(...,p)" y te debe dar 1. Esta verdad se conoce como el *pequeño teorema de Fermat* o *petit Fermat*. Fermat era francés, pero no es que fuera pequeño, sino que existe otro teorema de Fermat que tiene una historia cautivante y se le conoce como el *último teorema de Fermat*. Se mantuvo sin demostración por 350 años hasta 1993, cuando Andrew Wiles de Inglaterra logró dar una demostraciń correcta

Petit FERMAT: Si p es primo y $0 < a < p$ entonces $a^{p-1} \equiv 1(\text{mod } p)$

Ejercicio 6.1. (CALC) Verifica las siguientes potencias:

a) $5^{12}(\text{mod } 13)$ b) $4^{18}(\text{mod } 13)$ b) $3^{22}(\text{mod } 23)$

Ejemplo 6.1. Petit Fermat nos permite hallar otras potencias módulo p. Veamos $3^{90}(\text{mod } 23)$. Al dividir 90 por 22 (¿por qué 22?) obtenemos cociente 4 y residuo 12, es decir, $90 = 22 \times 4 + 2$, por lo que

$$3^{90}(\text{mod } 23) = 3^{22\times 4+2}(\text{mod } 23) = 3^{22\times 4} \times 3^2(\text{mod } 23) =$$

$$(3^{22})^4 \times 3^2(\text{mod } 23) = 1^4 \times 3^2(\text{mod } 23) = 9(\text{mod } 23) = 9$$

Ejercicio 6.2. Calcula las siguientes potencias:

a) $3^{40} (\text{mod } 11)$ b) $3^{40} (\text{mod } 13)$ c) $19^{200} (\text{mod } 47)$ d) $15^{1341402} (\text{mod } 101)$

Algo de notación. Antes de ver la próxima herramienta introduzcamos una notación para el número de invertibles de Z_N. Como recordarás estos son elementos que no comparten factores con N; se les llama *coprimos* de N. Al número de coprimos de N se le llama la función ϕ (se pronuncia 'fi') de Euler ('oiler', así como Freud) de N y se denota:

$$\phi_N = \textit{número de coprimos de } N, \textit{ menores que } N$$

Por ejemplo, los coprimos de 9, menores que 9 son $\{1, 2, 4, 5, 7, 8\}$; por tanto $\phi_9 = 6$. Conocemos bien a los coprimos de 27 y ellos son 18; por tanto $\phi_{27} = 18$. También $\phi_{101} = 100$ (¿correcto?)

En los Ejercicios 2.4, 2.5, 2.7 y 2.8 se hacen las mismas preguntas. Por el Ejercicio 2.7, para cualquier primo p, $\phi_p = p - 1$ y por el Ejercicio 2.8, para dos primos p y q, $\phi_{pq} = (p - 1)(q - 1)$

6.2. Teorema de Euler. En el ejercicio 2.10 se pedía demostrar que el producto de dos elementos invertibles a y b de Z_N es también invertible. Esto se puede justificar fácilmente porque si a y b no comparten factores con N, ab, que sólo tiene los factores de a y de b, tampoco tendrá factores comunes con N. También vale el argumento que $a^{-1}b^{-1}$ debe ser el inverso de ab, pues el producto $(ab)(a^{-1}b^{-1}) = 1$ (¿correcto?)

Entonces sucede lo que pensamos al explicar petit Fermat: cuando calculamos las superpotencias de un invertible $a \in Z_N$, multiplicamos a por sí mismo repetidas veces y recorremos los elementos invertibles de Z_N (finito) y eventualmente reencontraríamos al mismísimo elemento a. Es decir, tendría que haber un exponente e tal que $a^e = a$, en Z_N. Euler dice que ese exponente es $e = \phi_N$, el número de coprimos de N. Más formalmente:

EULER: Si $0 < a < N$ y $mcd(a, N) = 1$, entonces $a^{\phi_N} \equiv a (\text{mod } N)$

Notarás que petit Fermat es un caso particular de Euler. Basta observar que si p es primo, $\phi_p = p - 1$, (Ejercicio 2.7). En el capítulo 8 veremos todo el poder de petit Fermat y Euler como herramientas en la criptografía de clave pública. Es importante entender bien los ejemplos y resolver los problemas que siguen.

Ejemplo 6.2. Verifiquemos Euler para $N = 9$. Sabemos que $\phi_9 = 6$. Escogemos un número coprimo con 9, $a = 2$ por ejemplo. Entonces calculamos (CALC) $a^{\phi_9} = 2^6 = 64 \equiv 1 (\text{mod } 9)$. Puedes verificar lo mismo con los otros coprimos de 9 : 4,5,7,8.

Ejemplo 6.3. (CALC) Escogemos dos primos $p = 701$ y $q = 809$ y tomamos $N = p \times q = 701 \times 809 = 567109$. Por el ejercicio 2.8 sabemos que $\phi_N = (700 - 1) \times (809 - 1) = 565600$. Escogemos $a = 3008$. Verificamos lo siguiente:

i. Con INVRS, 3008 es invertible módulo 567109, es decir $mcd(3008, 567109) = 1$.

ii. Con POTNS, la potencia $3008^{565600} \equiv 1 (\text{mod } 567109)$, lo que verifica Euler.

Ejercicio 6.3. (CALC) Calcula las siguientes potencias. Explica de qué manera cada caso verifica el teorema de Euler.

a) $17^{17} (\text{mod } 32)$ b) $20^{61} (\text{mod } 77)$ c) $50^{73} (\text{mod } 91)$ d) $15^{1341402} (\text{mod } 101)$

Ejercicio 6.4. (CALC) Escoge dos primos de 3 ó más dígitos. Halla $N = pq$ y un elemento a coprimo con N. Calcula ϕ_N y también (INVRS) el inverso b de a modulo ϕ_N. Escoge un número P menor que N y evalúa:

$$(P^a)^b = P^{ab} (\text{mod } N)$$

Explica por qué obtuviste ese resultado

§7. GRANDES LIGAS

7.1. DES. En 1973, el gobierno de los Estados Unidos hizo una convocatoria pública para la producción de un sistema criptográfico que pudiera ser usado universalmente. La compañía IBM produjo entonces lo que se conoce como Data Encription Standard, o DES por sus siglas. Originalmente de propiedad del gobierno de los Estados Unidos, DES es ahora de dominio público, se puede comprar en el mercado y su fortaleza reside en un complejo sistema de encriptación y de generación de claves.

DES convierte cualquier texto llano en texto digital, es decir, cadenas de ceros y unos. Por lo general usa los códigos ASCII de los caracteres del alfabeto romano que usan la mayoría de los lenguajes humanos, español incluído. Cada código ASCII es de 1 byte que consiste de 8 "binary digits" o "bits". De esta forma un mensaje de n espacios se transforma en texto llano de $8n$ bits. DES entonces fracciona el texto llano en bloques de 56 bits a los que agrega 8 bits. Entonces a cada bloque de 64 bits le aplica 16 permutaciones que constituyen la clave. DES esta diseñado para que la clave de encriptar sea la misma de decriptar.

DES evoluciona y ha demostrado ser muy confiable. No se sabe que su clave haya sido quebrada por ningún criptoanalista. La matemática que respalda a DES no es objetivo de este módulo y nos ocuparemos de ella. Mencionamos DES porque es aparentemente el sistema de uso más generalizado. El lector interesado puede conseguir informacin en la bibliografía del Apéndice. La investigación en criptografía se mantiene muy activa y hay noticias del uso de mecánica cuántica para elaborar un sistema esperadamente inquebrable.

Con todo lo importante que es DES, se trata de un sistema de clave privada. Para usarlo, los comunicantes deben tener un contacto personal secreto en el que acordarán o intercambiarán la clave, salvo que usen otro sistema que permita el intercambio seguro de claves a través de canales públicos. Uno de esos sistemas es Diffie-Hellman del que nos ocuparemos más adelante, dentro de lo que es clave publica.

7.2. Clave pública. Para entender el concepto de *clave pública* imaginemos una instancia en que dos personas o entidades deban comunicarse secretamente, sabiendo que son objeto de cualquier tipo de espionaje. El teléfono, el correo, un mensajero o la Internet, son útiles para transmitir mensajes crípticos pero son impropios para transmitir claves. Emisor y receptor requieren por tanto de contacto personal y secreto en el que acordaran la clave. Contactos que pueden ser imprácticos por el volumen de comunicaciones (piensa en transferencias de dinero), la frecuencia de éstas, y las enormes distancias. Comunicación regular entre socios de negocios en diferentes países requerirá no sólo claves secretas, sino precavidas actualizaciones de esas claves.

Pero antes de entrar en los sistemas de clave pública mejoremos nuestra representacion numérica de las digrafías, que la necesitaremos más adelante.

7.3. Números de base 27. Con 27 caracteres en el alfabeto, podemos formar $27 \times 27 = 729$ digrafías ó 729 vectores (x, y). Si simplemente yuxtaponemos los componentes de los vectores para formar números podemos ir desde $0 = 00$ hasta 2626, distribuyendo, en un rango de 0 a 2,626 ([0...2626]) números (cero incluido), las pocas 729 digrafías que existen. Eso deja muchas brechas y en el momento de decriptar podríamos encontrarnos con números para los que no haya digrafía; 2328 es un ejemplo.

Una solución para eliminar las brechas es usar el sistema de numeración de base 27, similar a nuestro *sistema posicional* de base 10, y sirve no sólo para digrafías, sino para digrafías y otros paquetes de cualquier número de letras. Así como 345, en base 10, es

$$345 = 3 \times 10^2 + 4 \times 10 + 5$$

la trigrafía 'VEN', identificada con el vector (23,5,14)—coteja tabla TEN— en base 27 será:

$$VEN = 23 \times 27^2 + 5 \times 27 + 14 = 16916$$

Las digrafías, por ser de sólo dos símbolos, no necesitarán del término de las "centenas", las de la posición 27^2. Por ejemplo a "NO" le corresponde el vector $(14, 16)$, y por tanto el número $14 \times 27 + 16 = 394$, en la base 27. Así como hay exactamente $10^2 = 100$ (del 0 al 99) números de uno o dos dígitos decimales, en base 27 hay exactamente $27^2 = 729$ números de uno y dos "digitos". Y 729 es exactamente el número de digrafías. Por ello tenemos una correspondencia uno-a-uno entre las digrafías y los enteros en el rango de [0...728].

Tenemos entonces dos problemas, uno recíproco del otro:

1. Dada una digrafía, hallar el número que le corresponde en el rango [0...728]
2. Dado un número en el rango [0...728], qué digrafía le corresponde.

El primer problema ya lo hemos resuelto con la explicación anterior. El segundo problema lo trataremos como un ejemplo:

Ejemplo 7.1. Descubramos la digrafía, que corresponde al número 375. Sólo necesitamos escribir 375 como $x \cdot 27 + y$. Se ve que 'y' es el residuo de dividir por 27. Entonces usamos la calculadora para hallar $y = mod(375, 27) = 24$. Falta ahora el "dígito" de las "decenas". Para ello hacemos la resta $375 - 24 = 351$ y dividimos $y = 351 \div 27 = 13$. Entonces $375 = 13 \times 27 + 24$ que delata el vector $(13, 24)$ y por tanto la digrafía "MW"

Ejercicio 7.1. Halla el número que corresponde a las siguientes digrafías, y trigrafías

a) YO b) MU c) MUY b) ZIP

Ejercicio 7.2 Halla la palabra que corresponde a los siguientes números. No son sólo digrafías

a) 718 b) 1096 c) 257180

7.4. RSA (Rivest, Shamir y Adleman, sus creadores) En este sistema se usa una clave para encriptar y otra clave para decriptar. La seguridad se basa en la casi imposibilidad de deducir la clave de decriptar a partir de la clave de encriptar. Si Alicia (receptora genérica) espera recibir mensajes, entonces hace pública su clave C_E de encriptar (en un periódico o en su portal de Internet) y guarda secretamente su clave de decriptar C_D. Si Bernardo (emisor genérico) quiere enviar un mensaje a Alicia, toma la clave de encriptrar de Alicia, encripta el mensaje y despacha el texto críptico por medios públicos. Como sólo Alicia tiene la clave de decriptar, sólo ella puede leer el mensaje. La seguridad descansa en que para quebrar la clave hace falta *factorizar* un número gigantesco (200 o más dígitos) y no existe (aún) ningún algoritmo universal que lo haga. Irónicamente, depende, no de lo que sabemos, sino de lo que ignoramos.

Recuerda que factorizar significa descomponer en factores. Factorizar el 391 consiste en "descubrir" que 391 es el producto de los números primos 17 y 23, es decir $391 = 17 \times 23$. En general factorizar no es fácil; no existe un método o algoritmo suficientemente rápido. El método más común es la búsqueda exhaustiva de factores (Eratóstenes). La búsqueda se restringe a los números primos, y debe acabar cuando se haya alcanzado la raiz cuadrada del número (¿por que?). Aún con esta restricción encontrar los factores de un número muy grande, de 200 digitos por ejemplo, o descubrir que no los tiene, es una tarea que, con computadoras —sin duda— puede tomar varios años. El sistema criptográfico que vamos a describir, fundamenta su seguridad en la factorización. Si un critpoanalista necesita años para factorizar un número, el valor de la información que busca se habrá esfumado mucho antes.

Además de la noción de factorización, hay otros fundamentos matemáticos en los que se basa la critpografía de clave pública. Los discutiremos intuitivamente sin entrar en el rigor de sus demostraciones. Pero antes veamos cómo funciona RSA.

Generación de claves. En lo que sigue, Alicia será una receptora que hace pública su clave de encriptar. Como una figura importante cuya dirección es de conocimiento público, el Presidente por ejemplo, a quien cualquiera puede enviar mensajes directamente a su estafeta postal, de la que sólo él tiene la llave. Para generar sus claves, Alicia hace lo siguiente:

1. Obtiene dos números primos muy grandes p y q y los multiplica: $N = p \times q$. Este numero N tiene sólo los factores p y q. Un criptoanalista que tenga acceso a sólo N, pasará mucho trabajo para hallar p y q.

2. En $Z_N = \{0, 1, ..., (N-1)\}$ Alicia cuenta los elementos invertibles, como sabemos, aquéllos que no comparten factores con N. El total de éstos es $(p-1)(q-1)$ (¿por qué?. Véase Ejercicio 2.8). A este número lo llamamos $\phi_N = (p-1)(q-1)$.

3. Alicia entonces escoge un numero e entre 1 y ϕ_N que no comparta factores con ϕ_N; un primo que no lo divida bastará. Como ya sabemos este número e es invertible en Z_{ϕ_N} y Alicia calcula ese inverso, $d = e^{-1} (\mathrm{mod} \phi_N)$.

4. Alicia ahora crea dos claves: una de encriptar $C_E = (e, N)$ que hace pública. Otra de decriptar $C_D = (d, N)$ que guarda secretamente.

Mensaje en acción: Si Bernardo quiere enviar un mensaje a Alicia, convertirá el texto llano de su mensaje en un número $P < N$ (si el mensaje es largo, lo fracciona) y usa la clave de encriptar de Alicia, $C_E = (e, N)$, que está en Internet y (usa PWERS) calculará la potencia

$$Q = P^e (\mathrm{mod} N)$$

Transforma Q en texto alfabético (base 27) y obtiene el texto críptico alfabético W.

Alicia recibe W y fácilmente recupera Q (base 27), extrae su clave de decriptar $C_D = (d, N)$ y (con PWERS) calculará la potencia

$$Q^d (\mathrm{mod} N)$$

Como

$$Q^d = (P^e)^d = P^{ed} = P^1 = P, \tag{1}$$

Alicia ha hallado el número P original de Bernardo y, convertido a texto alfabético, leerá su texto llano.

Ejemplo 7.2. Rehagamos con números concretos los pasos de Alicia, Bernardo e Intruso:

Alicia en acción

1. Alicia escoge $p = 17$ y $q = 43$, ambos primos. Su producto $N = 731$
2. Calcula $\phi_N = (p-1)(q-1) = 16 \times 42 = 672$.
3. Escoge $e = 101$ (por ejemplo) entre 1 y $\phi_N = 672$, y como es primo, no comparte factores con 672 y es invertible en Z_{672}. El inverso de 101 en Z_{672} (INVERS) es $d = 173$.
4. Alicia entonces crea dos claves: de encriptar, $C_E = (101, 731)$, que hace pública [*www.malicia.net*] y de decriptar, $C_D = (173, 731)$, que guarda secretamente.

Bernardo en acción. Bernardo quiere enviar el mensaje "SI" a Alicia.

1. Convierte la digrafía SI en el vector (20,9) y luego al número correspondiente de base 27: $20 \times 27 + 9 = 549 = P$
2. Obtiene la clave de Alicia: $C_E = (101, 731)$ y (con POTNS) hace el cálculo:

$$Q = P^e = 549^{101} (\text{mod} 731) = 507 = 18 \times 27 + 21$$

   que identifica con el vector $(18, 21)$ y la digrafía "QT" que envía a Alicia.

Alicia de nuevo. Alicia recibe "QT"

1. Convierte la digrafía QT en el vector (18,21) y luego al número correspondiente de base 27: $18 \times 27 + 21 = 507$.
2. De su archivo secreto extrae su clave de decriptar: $K_D = (173, 731)$ y con el programa PWERS hace el cálculo:

$$Q^d = 507^{173} (\text{mod} 731) = 549 = 20 \times 27 + 9 = P$$

   que identifica con el vector $(20, 9)$ y la digrafía "SI". (Y sabe que Bernardo se casará con ella.)

Intruso en acción. Por medios ilícitos, Intruso captura el mensaje "QT" y conoce la clave de encriptar de Alicia $C_E = (101, 731)$. Sabe que QT corresponde al número 507, pero no conoce el exponente 173 de la clave secreta de Alicia. Para hallar el 173 debe conseguir el inverso de 101, módulo ϕ_{731}. Pero ϕ_{731} es el número de invertibles módulo 731. Lo puede conseguir de dos formas:

1. Cuenta cuántos números no tienen factores comunes con 731, pero como no conoce los factores de 731, no llegará muy lejos.

2. Decide factorizar 731. Eso es muy fácil si el número tiene tres cifras. No es nada fácil si el número tiene 400 cifras. (Llegará después de la boda.)

7.5. ¿Por qué funciona RSA? La respuesta directa es: Euler. Analicemos la cadena de igualdades (1) de la sección "Mensaje en acción"

$$Q^d = (P^e)^d = P^{ed} = P^1 = P$$

donde $ed \equiv 1 (\text{mod } \phi_N)$, por lo que $ed = k \cdot \phi_N + 1$, y por ello se obtiene la potencia

$$P^{ed} = P^{k\phi_N + 1} = (P^{\phi_N})^k \cdot P$$

y por Euler $P^{\phi_N} \equiv 1 (\text{mod } N)$, de donde $(P^{\phi_N})^k \equiv 1 (\text{mod } N)$ y por tanto

$$P^{ed} = P$$

Y eso explica por qué Alicia puede ver el mensaje texto llano de Bernardo.

Ejercicio 7.3. Usando la clave pública de encriptar de Alicia, $(e = 23561, N = 5541307)$, Bernardo le envía el siguiente mensaje;

$$AERRX\ BMPP\ GBUA\ BVJHJ$$

que tú, como intruso, interceptas. Sabes que Alicia tiene la debilidad de escoger sus números primos muy cercanos uno del otro. Con esa información, descifra el mensaje.

Ejercicio 7.4. (*Autenticidad*) Alicia ha recibido un mensaje que descifra y queda perpleja. No cree que sea Bernardo el autor de ese mensaje. Alguien, haciéndose pasar por Bernardo, ha tomado la clave pública de Alicia y le ha enviado un contrariante mensaje firmando falsamente como Bernardo.

Piensa, medita, discute y explica de qué manera podrías usar RSA para autenticar mensajes. Mejor dicho, qué podría hacer Bernardo para que Alicia tenga la garantía de que los mensajes de Bernardo son en efecto de Bernardo.

§8. INTERCAMBIO DE CLAVE: DIFFIE-HELLMAN

Confiable como es, la seguridad que ofrece RSA depende de hacer aritmética con números gigantescos, lo que determina comunicación muy lenta. Si los mensajes son documentos extensos, RSA resulta de poca utilidad. Es más fácil usar un sistema de clave privada pero rápido —DES es el favorito— y resolver el problema de intercambio de claves de otra manera. Ese problema fue resuelto por Diffie y Hellman en 1976. Su seguridad se basa en la dificultad de resolver el problema de *logaritmos discretos.*

8.1. Logaritmos discretos. Seguro que ya sabes que el logaritmo de 1000 en base 10 es 3. Este hecho lo puedes verificar en tu calculadora, pero me más interesa que sepas por qué ese logaritmo es 3. La razón es que $10^3 = 1000$. Podemos escribirlo en la notación habitual:

$$\log_{10} 1000 = 3 \quad \text{porque} \quad 10^3 = 1000$$

Logaritmo es sinónimo de *exponente.* Cada vez que vemos una potencia, desde otro ángulo veremos un logaritmo. Por ejemplo,

$$3^4 = 81 \qquad \text{es lo mismo que} \qquad log_3 81 = 4$$

En aritmética modular también tenemos logaritmos, siempre que el módulo p sea un número primo. Se apellidan *discretos* por oposición a los *continuos* que son los que conocemos; tiene que ver con la finitud del conjunto donde se definen.

Por ejemplo, para $p = 7$ (primo), $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$. Si ignoramos el 0 obtenemos

$$Z_7^* = \{1, 2, 3, 4, 5, 6\}$$

en el que se puede multiplicar cerradamente, sin salirse de Z_7^*. Es más, el número 3, por ejemplo, tiene la propiedad que todas sus potencias *cubren todo* Z_7^*. Es decir, cada elemento de Z_7^* es una potencia de 3 y por ello en Z_7^* tenemos un *logaritmo de base 3.* En efecto:

POTENCIA		LOGARITMO
$3^0 = 1$	$\rightarrow$	$log_3 1 = 0$
$3^1 = 3$	$\rightarrow$	$log_3 3 = 1$
$3^2 = 2$	$\rightarrow$	$log_3 2 = 2$
$3^3 = 6$	$\rightarrow$	$log_3 6 = 3$
$3^4 = 4$	$\rightarrow$	$log_3 4 = 4$
$3^5 = 5$	$\rightarrow$	$log_3 5 = 5$

Observa que $3^6 = 3^5 \times 3 = 5 \times 3 = 15 = 1 (\text{mod } 7)$ lo cual dice que después de cubrir Z_7^*, las potencias de 3 se repiten cíclicamente.

En todo este pareo hay una base fija que es 3 y cada elemento de Z_7^* tiene tiene un logaritmo en la base 3. No todo elemento sirve de base, como es el caso de 2 cuyas potencias no cubren todo Z_7^* (verifícalo). Cinco (5) en cambio sí puede ser base. En efecto:

$$(5^0, 5^1, 5^2, 5^3, 5^4, 5^5) = (1, 5, 4, 6, 2, 3)$$

Ejercicio 8.1. Halla todos los elementos que sirvan de base para logaritmos en Z_{11}^*

Estos elementos que puedan servir de base de logaritmos se llaman *generadores,* pues con sus potencias "generan" todo Z_p^*. Una propiedad de los números primos es que cada Z_p^* tiene al menos un generador, y a esta verdad le damos la importancia que merece:

$$\boxed{\text{Si } p \text{ es primo, existe } \alpha \in Z_p^* \text{ tal que } \{\alpha^n : n \textit{ entero}\} = Z_p^*}$$

Por ello si α es un generador de Z_p^*, todo elemento $x \in Z_p^*$ tiene un logaritmo de base α módulo p.

Ejercicio 8.2. Identifica generadores en

a) Z_{11}^* b) Z_{17}^* c) Z_{23}^*

Ejercicio 8.3. Halla los siguientes logaritmos:

a) En Z_{11}^*, $\log_3 5$ b) En Z_{11}^*, $\log_4 7$ c) En Z_{31}^*, $\log_3 2$

d) En Z_{31}^*, $\log_{11} 4$ e) En Z_{101}^*, $\log_3 6$

El problema de los logaritmos discretos. Al resolver lo ejercicios anteriores, especialmente 8.2 c), d), e) te habrás preguntado si existe alguń algortimo que permita hallar esos logaritmos más fácilmente. La respuesta es NO!. Se tiene que hacer por exhaución y mientras más grande sea el módulo, mayor será el tiempo que tome hallar el logaritmo. Otro problema es hallar un generador; pero de eso no nos ocuparemos. Existen tablas de primos y generadores.

La dificultad del cálculo de los logaritmos discretos da seguridad al esquema de intercambio de claves que diseñaron Diffie y Hellman.

8.2. Intercambio de claves Diffie-Hellman. En un sistema de clave privada como DES, la clave generalmente es una "palabra" que como sabemos tiene un correspondiente numérico

que podemos calcular usando la base de numeración 27 (Véase 7.3). Por tanto la clave es en realidad un número. Veremos cómo dos comunicantes pueden acordar un número secreto.

Acuerdo público en acción. A través de un medio público (Internet por ejemplo) Alicia y Bernardo se ponen de acuerdo en usar un número primo p muy grande y un generador G de Z_p^* (Intruso detecta ambos números). Alicia escoge un entero $a < p$ que usará como exponente y mantiene secreto. Bernardo hace lo propio, escoge un entero $b < p$ que usará como exponente y también mantiene secreto.

Intercambio de claves en acción. Con su exponente secreto Alicia calcula $G^a (\mathrm{mod}\, p)$ que envía a Bernardo (Intruso se entera). Bernardo por su parte calcula $G^b (\mathrm{mod}\, p)$ que envía a Alicia (Intruso se entera: ve los resultados de G^a y G^b, pero no ve a ni b).

Alicia recibe G^b y con su exponente secreto calcula $(G^b)^a$. Bernardo hace lo propio: recibe G^a y con su exponente secreto calcula $(G^a)^b$. Como

$$(G^b)^a = G^{ba} = G^{ab} = (G^a)^b = K,$$

Alicia y Bernardo comaparten el número K que nadie más conoce.

Intruso en acción. Intruso conoce G, G^a, y p. No conoce a. Tiene un problema de logaritmo discreto. Tendrá que recurrir a otros medios. Podría usar su computadora más veloz para calcular potencias sucesivas de G: G^2, G^3, G^4,... etcétera, hasta encontrar un exponente que le dé G^a. Si el primo p es de más de 200 dígitos, el proceso le puede tomar años.

Ejemplo 8.1. (CALC) Trabajemos a escala *microscópica* para entender bien este esquema. Alicia y Bernardo acuerdan usar el primo $p = 2003$ y el generador $G = 106$. Todo el mundo sabe que ellos usan $(p = 2003, G = 106)$.

Alicia escoge su exponente (cabalístico) $a = 381$, no se lo revela a nadie y calcula (POTNS)

$$G^a (\mathrm{mod}\ p) = 106^{381} (\mathrm{mod}\ 2003) = 1717,$$

y envía '1717′ a Bernardo.

Bernardo escoge su exponente (de buena suerte) $b = 751$, no lo revela a nadie y calcula

$$G^b (\mathrm{mod}\ p) = 106^{751} (\mathrm{mod}\ 2003) = 158$$

y le envía '158′ a Alicia.

Alicia, en secreto, hace el cálculo $\quad 158^{381} (\mathrm{mod}\ 2003) = 1193$

Bernardo, en secreto, hace el cálculo $1717^{7511} (\text{mod } 2003) = 1193$

y $K = 1193$ es la clave que comparten.

Intruso conoce $p = 2003$, el generador $G = 106$ y $G^a = 1717$. su problema es hallar

$$\log_{106} 1717 (\text{mod } 2003) \quad \acute{o} \quad \log_{106} 158 (\text{mod } 2003)$$

Con un número p de 4 cifras, CALC puede dar la respuesta, pero si p tuviera 200 cifras o más, el cálculo de cualquiera de los dos logaritmos sería muy costoso en términos de tiempo.

Ejercicio 8.1. (CALC) Estás de intruso. Navegas (*surfeas*) por los portales de Alicia y Bernardo y en ambos hallas ($p = 43, G = 18$). Luego ves el misterioso número 11 en la página de Bernardo y el misterioso número 15 en la página de Alicia. ¿Puedes determinar el número secreto que Alicia y Bernardo comparten?

BIBLIOGRAFIA

- BEUTELSPACHER, Albrecht, *Criptology*, The Mathematical Association of America, 1994, ISBN 0-88385-504-6
- KOBLITZ, Neal, *A Course in Number Theory and Criptography*, Second Edition, Springer-Verlag, 1994, ISBN 0-387-94293-9
- MENEZEZ, Alfred; vanOORSCHOT, Paul; SCOTT, Vanstone, *Handbook of Applied Criptogrphy*, CRC Press 1994, ISBN 0-8493-8523-7
- STINSON, Douglas, *Criptography, Theory and Practice*, CRC Press 1995, ISBN 0-8493-8521-0
- SIMMONS, Gustavus; editor, *Contemporary Criptology, The Science of Information Integrity*, IEEE Press, 1992, ISBN 0-87942-277-7

POTENCIAS

PROGRAM:POTNS
:Disp "modulo"
:Input M
:Disp "base"
:Input B
:Disp "exponente"
:Input E
:If $E == 1$
:Then
:B → P
:Else
:1 → P
:While $E > 1$
:While mod(E,2)==0
:mod(B^2, M) → B
:E/2 → E
:End
:mod(P*B,M)→ P
:$E - 1$ → E
:End
:End
:Disp P

BEZOUT

PROGRAM:BZOUT
:1 → A1
:1 → B
:0 → B1
:0 → A
:M → C
:N → D
:iPart(C/D) → Q
:mod(C,D)→ R
:If R==0
:Then
:D → U
:Else
:While R ≠ 0
:D → C
:R → D
:A1 → T
:A → A1
:T-Q*A → A
:B1 → T
:B → B1
:$T - Q * B$ → B
:iPart(C/D) → Q
:R → U
:mod(C,D)→ R
:End
:End

INVERSO

PROGRAM:INVRS
:Disp "modulo"
:Input M
:Disp "numero"
:Input N
:mod(M,N)→ N
:BZOUT
:If $U > 1$
:Then
:Disp "no invertible"
:Else
:If $B > 0$
:Then
:Disp B
:Else
:M+B → B
:Disp B
:End
:End

PRIMALIDAD

PROGRAM:PRIMO
:Disp "numero"
:Input M
:If $mod(M, 2) == 0$
:Then
:Goto N
:Else
:If $M \leq 7$
:Then
:Goto S
:Else
:3 → B
:While $B \leq \sqrt{M}$
:If $mod(M, B) == 0$
:Then
:Disp "FACTOR"
:Disp B
:Goto N
:Else
:B+2 → B
:End
:End
:Lbl S
:Disp "ES PRIMO"
;Goto A
:Lbl N
:Disp "NO PRIMO"
:End
:Lbl A