Guía de contenidos
para el
IV Torneo de Ciencias - 2023
CLAVEMAT EPN - MIC

Juan Carlos Trujillo

CLAVEMAT - Noviembre 2023

Introducción

Las tareas que deberás realizar incluyen los siguientes contenidos de matemática:

a. Álgebra básica.

b. Geometría básica.

c. El plano cartesiano.

d. Trigonometría.

e. Divisibilidad y aritmética modular básica.

f. Matrices cuadradas

Salvo el último tema, todos los demás aprendes en los tres últimos años de la Educación Básica y en los dos primeros del Bachillerato. Por esta razón, en este documento, encontrarás una guía general de los primeros cuatro contenidos y una presentación más detallada del último tema. También encontrarás una descripción detallada y algunos ejemplos del *criptosistema* RSA para cifrar y descifrar mensajes, y los métodos de encriptación de Vigenère y de Hill. Estos serán los protocolos que deberás aprender para resolver algunas de las tareas del Torneo.

Finalmente, la última sección contiene una guía sobre *triangulación*, necesaria para la solución de algunas tareas del Torneo.

Contenidos de Álgebra básica

i) Las **cuatro operaciones entre polinomios**: suma, resta, multiplicación y división.

ii) Potencias y radicales.

iii) Los denominados **productos notables** básicos: el producto de dos binomios, el cuadrado de un binomio, el cubo de un binomio, el binomio de Newton.

iv) La **descomposición en factores básica de polinomios**: diferencia de cuadrados y de cubos, trinomios.

v) Ecuaciones de primero y segundo grado con una incógnita.

vi) "Despeje" de fórmulas.

vii) Sistemas de dos y tres ecuaciones lineales.

viii) Inecuaciones (desigualdades) lineales con una o dos incógnitas.

Contenidos de Geometría básica

i) Clasificación de los triángulos respecto de sus lados o de sus ángulos: equiláteros, isósceles y escalenos.

ii) Rectas y segmentos especiales de los triángulos: alturas, medianas, mediatrices y bisectrices.

iii) Fórmulas generales para calcular el área de un triángulo, rectángulo, círculo, polígono, cilindro, cono y esfera.

iv) Fórmulas generales para calcular el volumen de un paralelepípedo, cilindro, cono y esfera.

v) El teorema de Pitágoras.

vi) La suma de las medidas de los ángulos internos de un triángulo.

Contenidos del plano cartesiano

i) Representación de cada punto del plano mediante un par ordenado de números reales.

ii) La fórmula para la distancia entre dos puntos en el plano.

iii) La ecuación de una recta.

iv) La ecuación de un círculo.

Contenidos de Trigonometría

i) Definición de las razones trigonométricas para los ángulos agudos de un triángulo rectángulo: seno, coseno, tangente, cotangente, secante y cosecante.

ii) Razones trigonométricas de los ángulos de 30, 45 y 60 grados.

iii) Identidades trigonométricas pitagóricas: $\operatorname{sen}^2\alpha + \cos^2\alpha = 1$, $1 + \tan^2\alpha = \sec^2\alpha$, $1 + \operatorname{cosec}^2\alpha$.

iv) Identidades trigonométricas básicas: razones trigonométricas del complemento de un ángulo, razón trigonométrica de un ángulo en función de las otras razones trigonométricas.

v) Razones trigonométricas de ángulos en un plano cartesiano (razones trigonométricas de los ángulos según el "cuadrante" en el que están).

vi) Razones trigonométricas de ángulos con medidas, 0, 90, 180, 270 y 360 grados y sus múltiplos.

vii) Razones trigonométricas de ángulos con medidas múltiplos de 30, 45 y 60.

viii) Razones trigonométricas de la suma y resta de ángulos, el ángulo doble, el ángulo mitad, del inverso aditivo de un ángulo (por ejemplo, $\operatorname{sen}(-\alpha) = -\operatorname{sen}\alpha$.

ix) La ley de senos y la ley de cosenos.

x) Fórmulas del área de un triángulo en términos de razones trigonométricas.

xi) Identidades trigonométricas sencillas.

Contenidos de divisibilidad y aritmética modular

Divisibilidad

Como el número 8 es igual al producto de 4 y 2,

$$8 = 4 \times 2,$$

decimos que 4 **divide** a 8 y que 2 **divide** a 8. Por esta misma razón, decimos que 3 y 4 dividen a 12, pues

$$12 = 4 \times 3.$$

Definición 1: Divide y divisible

Un número natural n **divide** a otro número natural m si el número m se expresa de la siguiente manera:

$$m = kn,$$

donde k es un número natural. Se escribirá

$$m \mid n$$

para indicar que m **divide** a n.

Así, podemos escribir

$$2 \mid 8, \quad 4 \mid 8, \quad 4 \mid 12.$$

Si m divide a n también diremos que n es **divisible** por m. Así, 8 es divisible por 2 y por 4; 12 es divisible por 3 y por 4, etcétera.

Ejemplos: Divisibilidad

1. El número 8 es divisible por 4 y por 2 porque

$$8 = 4 \times 2;$$

por tanto,

$$2 \mid 8 \quad y \quad 4 \mid 8.$$

2. El número 12 es divisible por 4 y por 3 porque

$$12 = 4 \times 3;$$

por tanto,

$$4 \mid 12 \quad y \quad 3 \mid 12.$$

3. El número 10 es divisible por 5 y por 2 porque

$$10 = 5 \times 2;$$

por tanto,

$$5 \mid 10 \quad y \quad 2 \mid 10.$$

4. El número 32 es divisible por 8 y por 4 porque

$$32 = 8 \times 4;$$

por tanto,

$$8 \mid 32 \quad y \quad 4 \mid 32.$$

5. **Todo número es divisible por sí mismo.** En efecto, si n es un número natural, tenemos que

$$n = 1 \times n;$$

por tanto, n es divisible por n. Y, por esta misma razón, n **es divisible por** 1.

Números primos

El número 8 se divide por 1, por 2, por 4 y por el mismo 8; es decir, el número 8 tiene cuatro divisores. El número 10 también tiene cuatro divisores: 1, 2, 5 y 10; el número 9 tiene tres: 1, 3 y 9. En cambio, el 7 tiene únicamente dos divisores: 1 y 7; lo mismo ocurre con el 5: sus únicos divisores son 1 y 5. Aquellos números cuyos divisores son únicamente el 1 y ellos mismos se denominan **números primos**; así, el 7 es un **número primo**.

Definición 2: Números primos

Un número natural n, distinto de 1, es un **número primo** si sus únicos divisores son 1 y n.

Ejemplo: Números primos

Los números primos menores que 100 son:

$$2,\ 3,\ 5,\ 7,\ 11,$$
$$13, 17, 19, 23, 29,$$
$$31, 37, 41, 43, 47,$$
$$53, 59, 61, 67, 71,$$
$$73, 79, 83, 89, 97.$$

Propiedad: Teorema fundamental de la Aritmética

Todo número natural es igual al producto de potencias de números primos.

Por ejemplo,

$$18 = 2 \times 3^2.$$

¿Por qué? Porque 18 se descompone en sus factores primos de la siguiente manera: si dividimos 18 por 2 -el primer número primo- tenemos 9 como cociente y 0 como residuo; si dividiéramos el cociente 9 por 2, el residuo ya no sería 0; por ello, ahora dividimos este cociente por el siguiente número primo: el 3; al hacerlo, obtenemos 3 como cociente y 0 como residuo; el nuevo cociente sí se divide por 3; lo hacemos y obtenemos 1 como cociente y, por ello, el proceso de descomposición termina. Así, podemos concluir que 18 es igual al producto de 2 (elevado a la potencia 1) y 3 a la potencia 2:

$$18 = 2 \times 3^2.$$

El procedimiento realizado puede ser resumido de la siguiente manera:

18	2
9	3
3	3
1	

Como puedes ver, en la columna de la izquierda, bajo el número 18, se escriben los cocientes que resultan de dividir por los números primos que se muestran en la columna de la derecha.

Ejemplos: Descomposición en factores primos

1. $500 = 2^2 \times 5^3$ porque

500	2
250	2
125	5
25	5
5	5
1	

2. $1107 = 3^3 \times 41$ porque

1107	3
369	3
123	3
41	41
1	

3. $1206 = 2 \times 3^2 \times 67$ porque

1206	2
603	3
201	3
67	67
1	

4. $1918 = 2 \times 7 \times 137$ porque

1918	2
959	7
137	137
1	

5. $2018 = 2 \times 1009$ porque

2018	2
1009	1009
1	

Máximo común divisor

Dados 8 y 12, ¿qué números dividen a los dos? Los números 2 y 4, ¿verdad? Efectivamente:

$$8 = 4 \times 2 \quad y \quad 12 = 6 \times 2$$

y

$$8 = 2 \times 4 \quad y \quad 12 = 3 \times 4.$$

Entre los dos números que dividen a 8 y al 12, el 4 es el más grande; a este número se le llama **máximo común divisor** de 8 y de 12 y se representa de la siguiente manera:

$$\text{mcd}(8, 12) = 4.$$

Definición 3: Máximo común divisor

Dados dos números enteros m y n, su **máximo común divisor** mcd es el número más grande que divide a m y n. Si p es el máximo común divisor de m y n, escribiremos así:

$$\text{mcd}(m, n) = p.$$

¿Cuál es el máximo común divisor de 18 y 216? Para hallar este número, bastaría con descomponer los dos números en factores primos y establecer cuál de estos divisores es el mayor número que divide a 18 y 216. Así:

$$18 = 2 \times 3^2$$

pues

18	2
9	3
3	3
1	

Ahora,

$$216 = 2^3 \times 3^3$$

pues

216	2
108	2
54	2
27	3
9	3
3	3
1	

Vemos que 1, 2, 3, 3^2 y 2×3^2 dividen a los números: 18 y 216, ¿verdad? Sin embargo, el divisor más grande de estos cinco números es el 2×3^2, es decir, 18. Por tanto,

$$\text{mcd}(18, 216) = 18.$$

Mediante este procedimiento siempre se puede hallar el máximo común divisor de dos números; no obstante, este procedimiento puede tomar mucho tiempo y esfuerzo si nos enfrentamos a dos números grandes; por ejemplo, 15940 y 435198. Por ello, vamos a recurrir a otro algoritmo descubierto uno de los matemáticos más destacado de todos los tiempos: el griego Euclides.

Propiedad: Algoritmo de Euclides para hallar el Máximo Común Divisor

Dados dos números enteros m y n y, suponiendo que m es mayor que n, su **máximo común divisor** se calcula del siguiente modo:

1. Dividimos m por n y hallamos su cociente y su residuo.
2. Si el residuo es mayor que 0, realizamos una nueva división, ahora del divisor por el residuo.
3. Repetimos este procedimiento hasta obtener 0 como residuo.

El **máximo común divisor** de los números m y n es el divisor de la última división realizada.

Ejemplo: Algoritmo de Euclides

¿Cómo calcularíamos el máximo común divisor de 5940 y 3528 utilizando el algoritmo de Euclides? Veamos:

1. Dividimos 5940 por 3518:

$$\begin{array}{r|l} 5940 & 3528 \\ \hline 2412 & 1 \end{array}$$

   Su cociente es 1 y su residuo es 2412.

2. Como el residuo 2412 es mayor que 0, realizamos una nueva división, ahora del divisor por el residuo. Así:

$$\begin{array}{r|l} 3528 & 2412 \\ \hline 1116 & 1 \end{array}$$

   Ahora el cociente es 1 y el residuo es 1116.

3. Repetimos el procedimiento anterior hasta obtener 0 como residuo:

$$\begin{array}{r|l} 2412 & 1116 \\ \cline{2-2} 180 & 2 \end{array}$$

$$\begin{array}{r|l} 1116 & 180 \\ \cline{2-2} 36 & 6 \end{array}$$

$$\begin{array}{r|l} 180 & 36 \\ \cline{2-2} 0 & 5 \end{array}$$

En resumen: 2412 dividido por 1116 es 2 con un residuo de 180, que es mayor que 0; luego, hay que volver a realizar una división: 1116 por 180; el cociente es 6 y el residuo, 36. Finalmente, al dividir 180 por 36, se obtiene como cociente 5 y residuo de 0.

Por tanto, el **máximo común divisor** es el último divisor, esto es 36. Así:

$$\text{mcd}(3528, 5940) = 36.$$

Ejemplos: Algoritmo de Euclides para calcular el Máximo Común Divisor

1. El $\text{mcd}(50, 13) = 5$, pues:
   (a) 135 dividido por 50 es 2, con residuo 35.
   (b) 50 dividido por 35 es 1, con residuo 15.
   (c) 35 dividido por 15 es 2, con residuo 5.
   (d) 15 dividido por 5 es 3, con residuo 0. El número 5 es el último divisor y, por tanto, es el **máximo común divisor** de 50 y de 1.
2. El $\text{mcd}(36, 200) = 4$, pues:
   (a) 200 dividido por 36 es 5, con residuo 20.
   (b) 36 dividido por 20 es 1, con residuo 16.
   (c) 20 dividido por 16 es 1, con residuo 4.
   (d) 16 dividido por 4 es 4, con residuo 0. El número 4 es el último divisor y, por tanto, el **máximo común divisor** de 36 y 200.
3. El $\text{mcd}(36, 200) = 4$, pues:
   (a) 200 dividido por 36 es 5, con residuo 20.
   (b) 36 dividido por 20 es 1, con residuo 16.
   (c) 20 dividido por 16 es 1, con residuo 4.

(d) 16 dividido por 4 es 4, con residuo 0. El número 4 es el último divisor y, por tanto, es el **máximo común divisor** de 36 y 200.

4. El $\text{mcd}(512, 2000) = 16$, pues:

   (a) 2000 dividido por 512 es 3, con residuo 464.

   (b) 512 dividido por 464 es 1, con residuo 48.

   (c) 464 dividido por 48 es 9, con residuo 32.

   (d) 48 dividido por 32 es 1, con residuo 16.

   (e) 32 dividido por 16 es 2, con residuo 0. El número 16 es el último divisor y, por tanto, es el **máximo común divisor** de 512 y 2000.

5. El $\text{mcd}(1000, 2048) = 8$, pues:

   (a) 2048 dividido por 1000 es 2, con residuo 48.

   (b) 1000 dividido por 48 es 20, con residuo 40.

   (c) 48 dividido por 40 es 1, con residuo 8.

   (d) 40 dividido por 8 es 5, con residuo 0. El número 8 es el último divisor y, por tanto, es el **máximo común divisor** de 1000 y 2048.

6. El $\text{mcd}(3528, 5940) = 36$, pues:

   (a) 5940 dividido por 3528 es 1, con residuo 2412.

   (b) 3528 dividido por 2412 es 1, con residuo 1116.

   (c) 2412 dividido por 1116 es 2, con residuo 180.

   (d) 1116 dividido por 180 es 6, con residuo 36.

   (e) 180 dividido por 36 es 5, con residuo 0. El número 36 es el último divisor y, por tanto, el **máximo común divisor** de 3528 y 5940.

Mínimo común múltiplo

Dados 8 y 12, ¿qué números, en común, son múltiplos de ellos? O, más bien dicho, 8 y 12, ¿a qué números dividen ambos? Podrían ser, por ejemplo, los números 24, 48 y 96, pues

$$8 \mid 24, \quad 8 \mid 48 \quad y \quad 8 \mid 96$$

al igual que

$$12 \mid 24, \quad 12 \mid 48 \quad y \quad 12 \mid 96.$$

El número múltiplo más pequeño de 8 y de 12 es 24. A este número se le llama **mínimo común múltiplo** de 8 y de 12 y se representa de la siguiente manera:

$$\text{mcm}(8, 12) = 24.$$

Definición: Mínimo común múltiplo

Dados dos números enteros m y n, su **mínimo común múltiplo** $\text{mcm}(m,n)$ es aquel número que, del conjunto de los múltiplos comunes, es el más pequeño.

Para encontrar el **mínimo común múltiplo** de dos números, procedemos a descomponer cada uno de ellos en sus factores primos correspondientes; luego, el **mínimo común múltiplo** es resultado de la multiplicación de todos los factores comunes y no comunes elevados a la mayor potencia. Por ejemplo, el $\text{mcm}(72,50)$ es 1800 pues, por un lado, si descomponemos el número 72 en sus factores primos, tenemos que $72 = 2^3 \times 3^2$:

72	2
36	2
18	2
9	3
3	3
1	

Y, por otro lado, si descomponemos el número 50 en sus factores primos, tenemos que $50=2 \times 5^2$:

50	2
25	5
5	5
1	

Finalmente, si tomamos los factores comunes y no comunes de 72 y 50 con su mayor exponente, tenemos que:

$$\text{mcm}(72,50) = 2^3 \times 3^2 \times 5^2 = 1\,800.$$

Ejemplos

1. El $\text{mcm}(30,15) = 30$, pues, por un lado, si descomponemos el número 30 en sus factores primos, tenemos que $30 = 2 \times 3 \times 5$:

30	2
15	3
5	5
1	

Y, por otro lado, si descomponemos el número 15 en sus factores primos, tenemos que $15 = 3 \times 5$:

15	3
5	5
1	

Finalmente, si tomamos los factores comunes y no comunes de 30 y 15 con su mayor exponente, tenemos que

$$\text{mcm}(30, 15) = 2 \times 3 \times 5 = 30.$$

2. El $\text{mcm}(16, 28) = 112$, pues, por un lado, si descomponemos el número 16 en sus factores primos, tenemos que $16=2^4$:

16	2
8	2
4	2
2	2
1	

Y, por otro lado, si descomponemos el número 28 en sus factores primos, tenemos que $28=2^2 \times 7$:

28	2
14	2
7	7
1	

Finalmente, si tomamos los factores comunes y no comunes de 16 y 28 con su mayor exponente, tenemos que el $\text{mcm}(16, 28) =$

$$2^4 \times 7 = 112.$$

3. El $\text{mcm}(27, 36) = 108$, pues, por un lado, si descomponemos el número 27 en sus factores primos, tenemos que $27=3^3$:

27	3
9	3
3	3
1	

Y, por otro lado, si descomponemos el número 36 en sus factores primos, tenemos que

$36=2^2 \times 3^2$:

36	2
18	2
9	3
3	3
1	

Finalmente, si tomamos los factores comunes y no comunes de 27 y 36 con su mayor exponente, tenemos que el mcm $(27, 36)$ =

$$2^2 \times 3^3 = 108.$$

Aritmética modular

Dados 7 y 2, es posible expresar el número 7 en términos del número 2 del siguiente modo:

$$7 = 3 \times 2 + 1,$$

donde 3 es el **cociente** de la división de 7 por 2, y 1 es el **residuo**.

Igualmente, dados los números naturales 29 y 19, es posible decir que 29 está en términos de 19 porque:

$$29 = 1 \times 19 + 10,$$

donde 1 es el cociente de la división de 29 por 19, y 10 es el residuo.

De manera general, tenemos la siguiente propiedad:

Propiedad: Teorema de la división

Si a y b son números enteros, existen dos únicos números q y r tales que

$$a = q \times b + r,$$

donde $0 \leq r < b$. El número q es el **cociente** de la división de a por b y r, el **residuo**.

Si

$$a = q \times b + r,$$

donde r es el residuo, escribimos

$$a \bmod b = r$$

y decimos que

*el **módulo** de a y b es r.*

Así,

$$29 \bmod 19 = 10,$$

pues

$$29 = 1 \times 19 + 10.$$

Definición: Módulo

El **módulo** de dos números enteros a y b es el residuo r que resulta de dividir a por b. El módulo de a y b se expresa del siguiente modo:

$$a \bmod b = r$$

Es importante notar que

*el **módulo de** a **y** b es, en general, diferente del **módulo de** b **y** a.*

En efecto, como vimos en el ejemplo, el **módulo de** 29 **y** 19 **es** 10; sin embargo, el **módulo de** 19 **y** 29 **es** 19, ya que

$$19 = 0 \times 29 + 19.$$

Si $a = b$, entonces obviamente sucede que

$$a \bmod b = b \bmod a,$$

pues el residuo de dividir a por b es 0; luego, tenemos que

$$a \bmod b = 0 \quad \text{y} \quad b \bmod a = 0.$$

En ningún otro caso es posible que

$$a \bmod b = b \bmod a,$$

si a y b sea diferentes. Así, de manera general, tenemos la siguiente propiedad:

Propiedad: La operación módulo no es conmutativa

Si a y b son dos números enteros diferentes, tenemos que

$$a \bmod b \neq b \bmod a.$$

En el último ejemplo, vimos que $19 \bmod 29 = 19$; es decir, es el número 19, que es menor que 29. Y esto siempre es verdadero: si $a < b$, entonces

$$a = 0 \times b + a;$$

luego, tenemos que $a \bmod b = a$.

Así, de manera general, tenemos la siguiente propiedad:

Propiedad

Si a y b son dos números naturales diferentes de 0 y $a < b$, entonces

$$a \bmod b = a.$$

Ejemplos: El módulo de dos números enteros

1. $28 \bmod 12 = 4$, pues
$$28 = 2 \times 12 + 4$$
donde 2 es el cociente de la división de 28 por 12 y 4 es el residuo.
2. $39 \bmod 12 = 3$, pues
$$39 = 3 \times 12 + 3$$
donde 3 es el cociente de la división de 39 por 12 y 3 es el residuo.
3. $24 \bmod 5 = 4$, pues
$$24 = 4 \times 5 + 4$$
donde 4 es el cociente de la división de 24 por 5 y 4 es el residuo.
4. $460 \bmod 360 = 100$, pues
$$460 = 1 \times 360 + 100$$
donde 1 es el cociente de la división de 460 por 360 y 100 es el residuo.
5. $405 \bmod 360 = 45$, pues
$$405 = 1 \times 360 + 45$$
donde 1 es el cociente de la división de 405 por 360 y 45 es el residuo.

Los ejemplos que se presentan a continuación son de mucha utilidad para comprender cabalmente la operación **módulo**.

Ejemplos: Ecuaciones sencillas

1. Como $2 < 3$, tenemos que $2 \bmod 3 = 2$; pero también tenemos que $5 \bmod 3 = 2$, ya que
$$5 = 1 \times 3 + 2.$$
Y también $8 \bmod 3 = 2$, ya que
$$8 = 2 \times 3 + 2.$$
Estos ejemplos, nos muestran que
$$2 \bmod 3 = 5 \bmod 3 = 8 \bmod 3;$$

es decir, nos muestra que hay al menos tres números que, al dividir por 3, el residuo es el número 2.

2. Del ejemplo anterior, surge la siguiente pregunta: ¿cuáles son todos los números enteros positivos (naturales) x que al dividir x por 3 el residuo es igual a 2? Es decir, queremos saber cuales son todos los números naturales x tales que satisfacen la siguiente igualdad:

$$x \bmod 3 = 2.$$

¿Cómo podemos hallar "todos los x"? Fácilmente si recurrimos a la definición de mod.

En efecto, cuando x se divide por 3, obtenemos el cociente (llamémoslo q) y el residuo debe ser igual a 2; esto significa que el número x se expresa en términos de 2 de la siguiente manera:

$$x = 3q + 2, \tag{1}$$

donde el número q es el cociente (que es un número entero).

Esto también significa que por cada "valor" que pueda tomar q como número entero, nos dará un valor de x. Por ejemplo, si $q = 0$, entonces

$$x = 0 \times 3 + 2 = 2.$$

En otras palabras, si $q = 0$, $x = 2$. Entonces (como vimos en el ejemplo anterior), x puede tomar el valor 2 para hacer verdadera igualdad

$$x \bmod 3 = 2.$$

Este es un resultado que ya conocíamos del ejemplo anterior. La diferencia ahora es que podemos "saber" cuáles son todos los posibles valores que puede tomar x con la ayuda de la igualdad (1): simplemente dando a q todos los posibles valores que puede tomar. Por ejemplo, si $q = 1$, el valor obtenido de x es: $x = 3 + 2 = 5$. Si $q = 2$, el resultado sería $x = 8$. Si $q = 3$, obtendríamos que $x = 11$, etcétera.

Más aún, q puede ser un entero negativo; por ejemplo, $q = -1$; en ese caso, tendríamos que

$$x = (-1) \times 3 + 2 = -3 + 2 = -1.$$

Ahora bien, si solo queremos saber los valores de x que sean enteros positivos, entonces nos bastará con tomar valores de q mayores o iguales que 0.

En resumen, todos los valores de x que satisfacen la "ecuación"

$$x \bmod 3 = 2$$

son los que se pueden calcular mediante la fórmula

$$x = 3q + 2,$$

"dando" a q todos los valores en los números naturales.

3. **¿Qué número, entre 50 y 60, al ser dividido por 11 da como residuo el número 10?**

   En otras palabras, buscamos todos los números naturales x, que cumplan con las condiciones $50 \leq x \leq 60$ y $x \bmod 11 = 10$.

   Para respondernos a esta pregunta, procedemos como en el ejemplo anterior. En efecto, sabemos que al dividir x por 11 hay un cociente q y el residuo es 10, que se relacionan mediante la siguiente igualdad:

   $$x = 11q + 10. \tag{2}$$

   A partir de esta igualdad, "asignando valores a q" podríamos encontrar el x que esté entre 50 y 60. Una manera alternativa más efectiva es proceder de la siguiente manera:

   $$\begin{aligned} 50 < x < 60 &\Leftrightarrow 50 < 11q + 10 < 60 \\ &\Leftrightarrow 50 - 10 < 11q < 60 - 10 \\ &\Leftrightarrow 40 < 11q < 50. \end{aligned}$$

   Es decir, necesitamos un valor de q tal que $11q$ esté entre 40 y 50. ¿Qué valor es? Claro que sí: $q = 4$, ya que $11q = 44$ y está entre 40 y 50.

   Entonces, el valor buscado de x se obtiene de (2) tomando $q = 4$:

   $$x = 11(4) + 10 = 54.$$

   Y, como podemos ver, 54 está entre 50 y 60, y al dividir por 11, el residuo es 10.

4. **¿Cuáles son los números tales que el módulo de 25 y dichos números es igual a 3?**

   En otras palabras, ¿cuáles son los números naturales x tales que $25 \bmod x = 3$?

   Como en el ejemplo anterior, para resolver este problema, recurrimos a la definición de módulo: al dividir 25 por x, obtenemos un cociente q y residuo 3; es decir:

   $$\begin{aligned} 25 \bmod x = 3 &\Leftrightarrow 25 = qx + 3 \\ &\Leftrightarrow 25 - 3 = qx \\ &\Leftrightarrow qx = 22. \end{aligned}$$

   Es decir, los números x que satisfacen la igualdad $25 \bmod x = 3$ son aquellos que multiplicados por un natural q debe ser igual a 22:

   $$qx = 22.$$

   ¿Qué significa esto? ¡Simplemente que x divide a 22! Y los números que lo hacen son 1, 2, 11 y 22. Ahora bien, podemos descartar los números 1 y 2. El primero, porque el residuo de dividir 25 por 1 es 0; el segundo porque el residuo es 1.

   Nos quedan dos posibilidades: 11 o 22. Tenemos que:

   $$25 \bmod 11 = 3 \quad \text{y} \quad 25 \bmod 22 = 3.$$

   Por tanto, los números buscados son 11 y 22.

5. **¿Cuál es el número que al dividir entre 8 y él mismo el residuo es ese número?**

   En otras palabras, buscamos el número x tal que

   $$8 \bmod x = x.$$

   Y, para encontrarlo, como en los ejemplos anteriores, recurrimos a la definición de módulo, por lo que, al dividir 8 por x, se obtiene un cociente q y el residuo x:

   $$8 \bmod x = x \Leftrightarrow 8 = qx + x.$$

   Esto quiere decir que el x buscado debería satisfacer la igualdad

   $$8 = qx + x.$$

   Pero este es imposible, porque el residuo siempre tiene que ser menor que el dividendo; es decir, x (que es el residuo) debe ser menor que el dividendo, que también es x. Pero $x = x$ y no es cierto que $x < x$.

   El significado de esto es que no hay un número que satisfaga la igualdad $8 \bmod x = x$. En otras palabras, el problema no tiene solución.

Operaciones modulares

El cálculo efectivo del módulo de dos números puede resultar "largo", incluso para una calculadora electrónica, cuando los números son grandes. La siguiente propiedad permite simplificar ese cálculo en estos casos.

Propiedad: Módulo de una multiplicación

El módulo de ab y n puede expresarse del siguiente modo:

$$(ab) \bmod n = ([a \bmod n] \times [b \bmod n]) \bmod n.$$

Así:

$$\begin{aligned}(5 \times 4) \bmod 3 &= ([5 \bmod 3] \times [4 \bmod 3]) \bmod 3 \\ &= (2 \times 1) \bmod 3 \\ &= 2 \bmod 3 \\ &= 2.\end{aligned}$$

Propiedad: Módulo de potencias

El módulo de a^{p+q} y n puede descomponerse de la siguiente manera:

$$\begin{aligned} a^{p+q} \bmod n &= (a^p \times a^q) \bmod n \\ &= ([a^p \bmod n] \times [a^q \bmod n]) \bmod n. \end{aligned}$$

Así:

$$\begin{aligned} 22^{13} \bmod 77 &= 22^{6+7} \bmod 77 \\ &= \left(22^6 \times 22^7\right) \bmod 77 \\ &= \left(\left[22^6 \bmod 77\right] \times \left[22^7 \bmod 77\right]\right) \bmod 77 \\ &= (22 \times 22) \bmod 77 \\ &= 22^2 \bmod 77 \\ &= 22. \end{aligned}$$

Ejemplos

1. $24 \bmod 5 = 4$ pues:

$$\begin{aligned} 24 \bmod 5 &= (3 \times 8) \bmod 5 \\ &= ((3 \bmod 5) \times (8 \bmod 5)) \bmod 5 \\ &= (3 \times 3) \bmod 5 \\ &= 9 \bmod 5 \\ &= 4. \end{aligned}$$

2. $8^7 \bmod 5 = 2$ pues:

$$\begin{aligned} 8^7 \bmod 5 &= (8^4 \times 8^3) \bmod 5 \\ &= ((8^4 \bmod 5) \times (8^3 \bmod 5)) \bmod 5 \\ &= (4096 \bmod 5) \times (512 \bmod 5) \bmod 5 \\ &= (1 \times 2) \bmod 5 \\ &= 2 \bmod 5 \\ &= 2. \end{aligned}$$

3. $6^4 \bmod 5 = 1$ pues:

$$\begin{aligned} 6^4 \bmod 5 &= (6^2 \times 6^2) \bmod 5 \\ &= ((6^2 \bmod 5) \times (6^2 \bmod 5)) \bmod 5 \end{aligned}$$

$$= (36 \bmod 5) \times (36 \bmod 5) \bmod 5$$
$$= (1 \times 1) \bmod 5$$
$$= 1 \bmod 5$$
$$= 1.$$

4. $4^5 \bmod 7 = 2$ pues:

$$4^5 \bmod 7 = (4^2 \times 4^3) \bmod 7$$
$$= ((4^2 \bmod 7) \times (4^3 \bmod 7)) \bmod 7$$
$$= (16 \bmod 7) \times (64 \bmod 7) \bmod 7$$
$$= (2 \times 1) \bmod 7$$
$$= 2 \bmod 7$$
$$= 2.$$

5. $9^3 \bmod 3 = 0$ pues:

$$9^3 \bmod 3 = (9^2 \times 9^1) \bmod 3$$
$$= ((9^2 \bmod 3) \times (9^1 \bmod 3)) \bmod 3$$
$$= (81 \bmod 3) \times (9 \bmod 3) \bmod 3$$
$$= (0 \times 0) \bmod 3$$
$$= 0 \bmod 3$$
$$= 0.$$

6. $69 \bmod 4 = 1$ pues:

$$69 \bmod 4 = (3 \times 23) \bmod 4$$
$$= ((3 \bmod 4) \times (23 \bmod 4)) \bmod 4$$
$$= (3 \bmod 4) \times (3 \bmod 4) \bmod 4$$
$$= (3 \times 3) \bmod 4$$
$$= 9 \bmod 4$$
$$= 1.$$

7. $7^5 \bmod 8 = 7$ pues:

$$7^5 \bmod 8 = (7^3 \times 7^2) \bmod 8$$
$$= ((7^3 \bmod 8) \times (7^2 \bmod 8)) \bmod 8$$
$$= ((343 \bmod 8) \times (49 \bmod 8)) \bmod 8$$
$$= (7 \times 1) \bmod 8$$
$$= 7 \bmod 8$$
$$= 7$$

Uso del Excel para calcular el módulo de una multiplicación entre números "grandes"

¿Cómo calculamos $157^5 \bmod 4$? ¿El número 157^5 es grande, verdad? Si aplicamos las propiedades del módulo de la multiplicación y de las potencias, podríamos descomponer dicho número del siguiente modo:

$$\begin{aligned} 157^{3+2} \bmod 4 &= (157^3 \times 152^2) \bmod 4 \\ &= ((157^3 \bmod 4) \times (157^2 \bmod 4)) \bmod 4. \end{aligned}$$

Aún así, $157^3 \bmod 4$ y $157^2 \bmod 4$ siguen siendo operaciones muy grandes. ¿Cómo podríamos calcular ágilmente estas operaciones?

Vamos a recurrir a la aplicación Excel. Es muy sencillo:

1. Para calcular $157^3 \bmod 4$, colocamos, en una celda cualquiera, la siguiente fórmula:
   = RESIDUO(POTENCIA(157; 3); 4).
   El resultado es 1
2. Igualmente, para calcular $157^2 \bmod 4$, colocamos, en una celda cualquiera, la siguiente fórmula:
   = RESIDUO(POTENCIA(157; 2); 4). El resultado es 1

Por tanto,

$$\begin{aligned} 157^{3+2} \bmod 4 &= (157^3 \times 152^2) \bmod 4 \\ &= ((157^3 \bmod 4) \times (157^2 \bmod 4)) \bmod 4 \\ &= (1 \times 1) \bmod 4 \\ &= 1 \end{aligned}$$

Ejemplos: Cálculo del módulo de una multiplicación en Excel

1. $239^9 \bmod 7 = 1$ pues:

$$\begin{aligned} &239^{5+4} \bmod 7 \\ &\quad = (239^5 \times 239^4) \bmod 7 \\ &\quad = ((239^5 \bmod 7) \times (239^4 \bmod 7)) \bmod 7 \end{aligned}$$

En Excel, calculamos $239^5 \bmod 7$ y $239^4 \bmod 7$ del siguiente modo:

= RESIDUO(POTENCIA(239;5);7) = 1
= RESIDUO(POTENCIA(239;4);7) = 1

Por tanto:

$$((239^5 \bmod 7) \times (239^4 \bmod 7)) \bmod 7$$

$$= (1 \times 1) \bmod 7$$
$$= 1 \bmod 7$$
$$= 1$$

2. $2123^5 \bmod 3 = 2$ pues:

$$2123^{2+3} \bmod 3 = (2123^2 \times 2123^3) \bmod 3$$
$$= ((2123^2 \bmod 3) \times (2123^3 \bmod 3)) \bmod 3$$

En Excel, calculamos $2123^2 \bmod 3$ y $2123^3 \bmod 3$ del siguiente modo:

= RESIDUO(POTENCIA(2123;2);3) = 1
= RESIDUO(POTENCIA(2123;3);3) = 2

Por tanto:

$$((2123^2 \bmod 3) \times (2123^3 \bmod 3)) \bmod 3 = (1 \times 2) \bmod 3$$
$$= 2 \bmod 3$$
$$= 2$$

La operación módulo para los enteros negativos

Podemos extender la operación módulo a los enteros negativos de la siguiente manera:

Definición: Módulo para enteros negativos

El **módulo** de un entero negativo a y un entero positivo b es 0 si el módulo de $-a$ y b es 0; en el caso contrario, es la diferencia entre b y el módulo de $-a$ y b:

$$a \bmod b = \begin{cases} 0 & \text{si } (-a) \bmod b = 0, \\ b - ((-a) \bmod b) & \text{si } (-a) \bmod b \neq 0. \end{cases}$$

Ejemplos: Módulo para enteros negativos

1. $(-12) \bmod 5 = 3$, ya que:

$$12 \bmod 5 = 2 \neq 0,$$

de donde, obtenemos:

$$(-12) \bmod 5 = 5 - 2 = 3.$$

2. $(-100) \bmod 5 = 0$, porque

$$100 \bmod 5 = 0.$$

Una de las aplicaciones más importantes de los números enteros y del álgebra modular se encuentra en la *Criptografía* y en el **Criptoanálisis**.

Matrices cuadradas de números reales

Definición: Matriz cuadradas

Una **matriz cuadrada** es un arreglo de números en dos filas y en dos columnas:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}.$$

Las **filas** de esta matriz son los

$$\begin{pmatrix} a_{11} & a_{12} \end{pmatrix} \quad \text{y} \quad \begin{pmatrix} a_{21} & a_{22} \end{pmatrix}.$$

Las columnas son:

$$\begin{pmatrix} a_{11} \\ a_{21} \end{pmatrix} \quad \text{y} \quad \begin{pmatrix} a_{12} \\ a_{22} \end{pmatrix}.$$

Ejemplos: Matrices cuadradas

1. Los siguientes arreglos son matrices cuadradas:

$$\begin{pmatrix} 1 & -1 \\ 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{y} \quad \begin{pmatrix} 2 & 0 \\ 0 & -3 \end{pmatrix}.$$

2. Las filas de la primera matriz del ejemplo anterior son:

$$\begin{pmatrix} 1 & -1 \end{pmatrix} \quad \text{y} \quad \begin{pmatrix} 2 & 1 \end{pmatrix}.$$

Las columnas de la tercerea matriz del ejemplo anterior son:

$$\begin{pmatrix} 2 \\ 0 \end{pmatrix} \quad \text{y} \quad \begin{pmatrix} 0 \\ -3 \end{pmatrix}.$$

Definición: Producto de una fila y una matriz

Si

$$\begin{pmatrix} u & v \end{pmatrix}$$

es la fila de una matriz, el **producto de la esta fila por la matriz**

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

es la fila siguiente:

$$\begin{pmatrix} u & v \end{pmatrix}\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} ua_{11}+va_{21} & ua_{12}+va_{22} \end{pmatrix}.$$

Ejemplos: Producto de una fila y una matriz

1.

$$\begin{pmatrix} 2 & 3 \end{pmatrix}\begin{pmatrix} -3 & 4 \\ 2 & 7 \end{pmatrix} = \begin{pmatrix} (2)(-3)+(3)(2) & (2)(4)+(3)(7) \end{pmatrix} = \begin{pmatrix} 0 & 31 \end{pmatrix}.$$

2.

$$\begin{pmatrix} -4 & 5 \end{pmatrix}\begin{pmatrix} 12 & 0 \\ -27 & 8 \end{pmatrix} = \begin{pmatrix} (-4)(12)+(5)(-27) & (-4)(0)+(5)(8) \end{pmatrix} = \begin{pmatrix} -183 & 40 \end{pmatrix}.$$

La matriz inversa

Cuando se habla de una "inversa" de una operación dada, pensamos en una operación que "deshace" lo que hace la operación dada. Por ejemplo, en la multiplicación de números, si a 4 se multiplica 5, obtenemos el 20; luego, para "deshacer" dicha multiplicación, a 20 dividimos por 5; en este caso, la operación inversa es la "división".

Aunque la división parece una operación diferente de la multiplicación, en realidad, es una multiplicación "disfrazada": el proceso de dividir por 5 no es más que el proceso de multiplicar 20 por el "inverso" de 5, que es el número $\frac{1}{5}$:

$$r \cdot \frac{1}{r} = 1.$$

Por ejemplo:

$$4 \cdot 5 = 20 \quad \text{y} \quad 20\left(\frac{1}{5}\right) = 4.$$

La multiplicación de una fila y una matriz

$$vA$$

también puede ser "revertida" ("invertida") si encontramos una matriz, a la que llamaremos **inversa de** A, tal que

$$(vA)A^{-1} = v.$$

No siempre existirá la matriz A^{-1}. Veamos un ejemplo.

Ejemplo: Matriz inversa

Si

$$v = (-6 \quad 12) \quad \text{y} \quad A = \begin{pmatrix} -9 & 11 \\ 8 & -8 \end{pmatrix},$$

la matriz

$$\begin{pmatrix} \frac{1}{2} & \frac{11}{16} \\ \frac{1}{2} & \frac{9}{16} \end{pmatrix}$$

es la inversa de A, porque:

$$\begin{aligned} vA &= (-6 \quad 12)\begin{pmatrix} -9 & 11 \\ 8 & -8 \end{pmatrix} \\ &= [(-6)(-9) + (12)(8), (-6)(11) + (12)(-8)] \\ &= (150 \quad -162), \end{aligned}$$

luego:

$$\begin{aligned} (vA)(A^{-1}) &= (150 \quad -162)\begin{pmatrix} \frac{1}{2} & \frac{11}{16} \\ \frac{1}{2} & \frac{9}{16} \end{pmatrix} \\ &= \left((150)\left(\frac{1}{2}\right) + (-162)\left(\frac{1}{2}\right), (150)\left(\frac{11}{16}\right) + (-162)\left(\frac{9}{16}\right)\right) \\ &= (-6 \quad 12) \\ &= v. \end{aligned}$$

¿Cálculo de la matriz inversa de una matriz de orden 2?

Dada la matriz

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22}, \end{pmatrix}$$

si

$$|A| = a_{11}a_{22} - a_{21}a_{22} \neq 0,$$

entonces

$$A^{-1} = \begin{pmatrix} \frac{a_{22}}{|A|} & -\frac{a_{12}}{|A|} \\ -\frac{a_{21}}{|A|} & \frac{a_{11}}{|A|}. \end{pmatrix}$$

El número $|A|$ se denomina **determinante de la matriz** A.

Ejemplo: Cálculo de la inversa de una matriz

Si

$$A = \begin{pmatrix} -9 & 11 \\ 8 & -8 \end{pmatrix},$$

entonces

$$|A| = (-9)(-8) - (8)(11) = -16 \neq 0.$$

Por tanto:

$$A^{-1} = \begin{pmatrix} \frac{-8}{-16} & -\frac{11}{-16} \\ -\frac{8}{-16} & \frac{-9}{-16} \end{pmatrix}$$

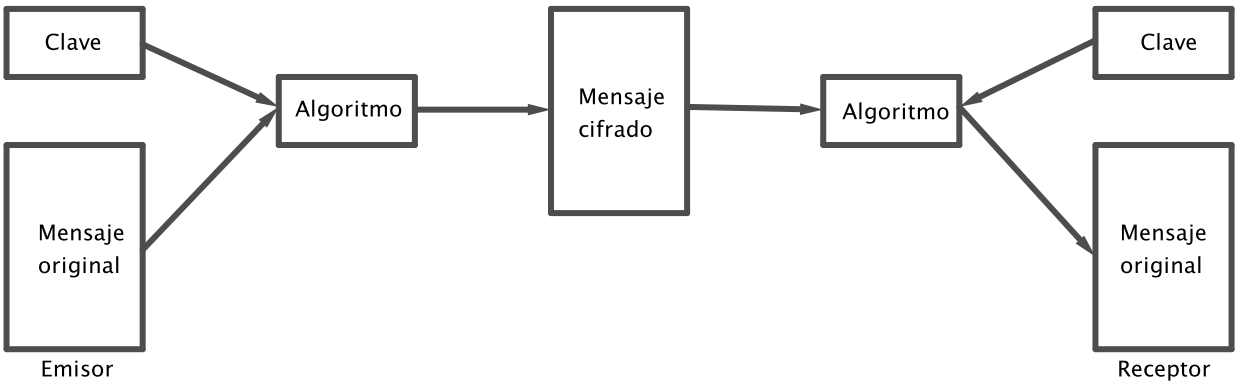
$$= \begin{pmatrix} \frac{1}{2} & \frac{11}{16} \\ \frac{1}{2} & \frac{9}{16}. \end{pmatrix}$$

Criptología

La *criptología* es un campo de estudio que, principalmente, desarrolla métodos para ocultar el significado de un mensaje que deberá ser enviado de manera segura por una persona, llamada generalmente **emisor**, a otra persona, denominada **receptor**. Que el envío sea seguro quiere decir que nadie, excepto el emisor y el receptor, puede averiguar el contenido del mensaje. En otras palabras, en el caso de que durante el viaje desde el emisor al receptor, el mensaje sea interceptado por una persona no autorizada, esta no podrá averiguar su contenido.

Para lograr esto, el emisor deberá sustituir las letras del texto original del mensaje por otras letras o números. El resultado de esta sustitución se denomina **texto cifrado** y la acción de sustitución se llama **cifrar** o **encriptar**. Cuando el mensaje cifrado llega finalmente al receptor, este podrá recobrar el mensaje original mediante la acción de **descifrar** el mensaje. El procedimiento para cifrar y descifrar un mensaje se conoce con el nombre de **algoritmo** o **protocolo**. Tanto para cifrar el mensaje original como descifrar el mensaje codificado, el emisor y el receptor requerirán de una o varias palabras secretas, denominadas **clave**. Una parte de esta clave puede ser de conocimiento público, pero una parte de ella deberá permanecer secreta.

El siguiente gráfico ilustra el proceso general que se sigue para el envío de un mensaje mediante la criptología:



A continuación, vamos a presentar uno de los *protocolos* para cifrar y descifrar mensajes. Este algoritmo pertenece a la categoría de protocolos de **clave pública**, porque una parte de la clave que requiere el emisor para cifrar el mensaje y enviarlo es de conocimiento público. Por supuesto, aquella parte que se requiere para descifrar el mensaje es secreta; el único que la conoce es el receptor. Después presentaremos también el método de Vigenère.

Algoritmo RSA

En 1978, Rivest, Shamir y Adleman publicaron el siguiente *criptosistema* de clave pública, denominado *RSA*.

El protocolo de ejecución del RSA

El procedimiento para su ejecución es el siguiente:

1. El **receptor** publica su clave pública que consta de dos números:

$$(n, r).$$

2. El **emisor** convierte cada letra y espacio en blanco del mensaje *M* (que enviará al **receptor**) en un número, utilizando las siguientes sustituciones:

Letra	Código	Letra	Código	Letra	Código
A	01	J	10	R	19
B	02	K	11	S	20
C	03	L	12	T	21
D	04	M	13	U	22
E	05	N	14	V	23
F	06	Ñ	15	W	24
G	07	O	16	X	25
H	08	P	17	Y	26
I	09	Q	18	Z	27
Espacio: 00					

El mensaje queda convertido en un número de la forma

$$\mathscr{M} = M_1 M_2 M_3 \dots M_K,$$

donde cada uno de los M_i es uno de los números entre 00 y 27 para todo $i \in \{1, 2, \dots, K\}$.

3. El **emisor** toma cada número M_i (con $i \in \{1, 2, 3, \dots, K\}$) y le *codifica* así:

$$R_i = M_i^r \bmod n$$

y envía al **receptor** el *mensaje codificado*

$$\mathscr{R} = R_1 R_2 R_3 \cdots R_K.$$

4. El **receptor** recibe el mensaje codificado $\mathscr{R}$ y le *decodifica* así:

$$M_i = R_i^s \bmod n$$

y obtiene el mensaje original, representado como un número:

$$\mathscr{M} = M_1 M_2 M_3 \cdots M_K.$$

5. El **receptor** recupera el mensaje original convirtiendo M al texto original utilizando una vez más la tabla de asignaciones numéricas a las letras y espacio:

Letra	Código	Letra	Código	Letra	Código
A	01	J	10	R	19
B	02	K	11	S	20
C	03	L	12	T	21
D	04	M	13	U	22
E	05	N	14	V	23
F	06	Ñ	15	W	24
G	07	O	16	X	25
H	08	P	17	Y	26
I	09	Q	18	Z	27
Espacio: 00					

Y, obtiene, finalmente, el mensaje original M.

Tareas previas a la ejecución del criptosistema RSA

El **receptor** es quien construye la **clave pública** (n, r) de la siguiente manera:

1. Elige al azar dos números primos p y q y toma n como el producto de p y q:

$$n = pq.$$

2. A continuación, con el fin de definir r, calcula el mínimo común múltiplo de $p-1$ y $q-1$, al que llama m:

$$m = \text{mcm}(p-1, q-1).$$

3. El número r es cualquier número entre 1 y m de manera que r y m sean primos entre sí, es decir, tales que el máximo común divisor de r y m sea iguala a 1:

$$\text{mcd}(r, m) = 1.$$

Además, el **receptor** deberá determinar el número s que le permitirá decodificar el mensaje que recibirá por parte del **emisor**; este número debe cumplir la propiedad

$$(rs) \bmod m = 1.$$

Para encontrarlo, el **receptor** calcula los números $r^2 \bmod m$, $r^3 \bmod m$, ..., hasta que $r^t \bmod m = 1$; entonces s es:

$$s = r^{t-1} \bmod m.$$

El número s debe permanecer en **secreto**.

Ejemplos: Protocolo RSA

1. Imaginemos que el **Emisor** va a enviar al **Receptor** es siguiente mensaje:

$$\texttt{SOL Y LUNA}$$

Para ello, sigue el protocolo siguiente.

P1: Consulta la **clave pública** del **emisor**:

$$(n, r).$$

Esta es

$$(77, 7);$$

es decir, sabe que $n = 77$ y $r = 7$.

P2: Convierte el mensaje

$$M = \texttt{SOL Y LUNA}$$

en el número

$$\mathscr{M} = M_1 M_2 M_3 \dots M_{10},$$

utilizando la siguiente tabla de sustituciones:

Letra	Código	Letra	Código	Letra	Código
A	01	J	10	R	19
B	02	K	11	S	20
C	03	L	12	T	21
D	04	M	13	U	22
E	05	N	14	V	23
F	06	Ñ	15	W	24
G	07	O	16	X	25
H	08	P	17	Y	26
I	09	Q	18	Z	27
Espacio: 00					

A la S le corresponde "20", a la O el "16", a la L el "12", al espacio en blanco el "00", a la Y el "26", al espacio en blanco el "00", a la L el "12", a la U el "22", a la N el "14" y, finalmente, a la A el "01"; es decir, el **emisor** obtiene que

$$M_1 = 20$$
$$M_2 = 16$$

$$M_3 = 12$$
$$M_4 = 00$$
$$M_5 = 26$$
$$M_6 = 00$$
$$M_7 = 12$$
$$M_8 = 22$$
$$M_9 = 14$$
$$M_{10} = 01.$$

Por tanto, el número que representa al mensaje es

$$\mathscr{M} = 20161200260012221401.$$

P3: El **emisor** toma cada número M_i (con $i \in \{1, 2, 3, \ldots, 10\}$) y le *codifica* así:

$$R_i = M_i^r \bmod n.$$

Como $n = 77$ y $r = 7$, el **emisor** procede de la siguiente forma:

$$\begin{aligned}
R_1 &= M_1^7 \bmod 77 \\
&= 20^7 \bmod 77 \\
&= 48. \\
R_2 &= M_2^7 \bmod 77 \\
&= 16^7 \bmod 77 \\
&= 58. \\
R_3 &= M_3^7 \bmod 77 \\
&= 12^7 \bmod 77 \\
&= 12. \\
R_4 &= M_4^7 \bmod 77 \\
&= 0^7 \bmod 77 \\
&= 00. \\
R_5 &= M_5^7 \bmod 77 \\
&= 26^7 \bmod 77 \\
&= 05. \\
R_6 &= M_6^7 \bmod 77 \\
&= 0^7 \bmod 77 \\
&= 00. \\
R_7 &= M_7^7 \bmod 77 \\
&= 12^7 \bmod 77 \\
&= 12.
\end{aligned}$$

$$
\begin{aligned}
R_8 &= M_8^7 \bmod 77 \\
&= 22^7 \bmod 77 \\
&= 22. \\
R_9 &= M_9^7 \bmod 77 \\
&= 14^7 \bmod 77 \\
&= 42. \\
R_{10} &= M_{10}^7 \bmod 77 \\
&= 1^7 \bmod 77 \\
&= 01.
\end{aligned}
$$

Obtiene así el mensaje codificado

$$\mathscr{R} = R_1 R_2 \cdots R_{10} = 48581200050012224201,$$

que es el que envía al **receptor**.

P4: El **receptor** recibe el mensaje codificado $\mathscr{R}$ y le *decodifica* así:

$$M_i = R_i^s \bmod n.$$

Para obtener cada uno de los M_i, el **receptor** necesita disponer del número s; este es secreto y, justamente, él es el único que lo conoce. En este caso $s = 13$ (en breve, explicaremos cómo el **receptor** determina su clave pública (n, r) y cómo obtiene el número secreto s) y la decodificación sucede así:

$$
\begin{aligned}
M_1 &= R_1^{13} \bmod 77 \\
&= 48^{13} \bmod 77 \\
&= 48^{6+7} \bmod 77 \\
&= \left(48^6 \times 48^7\right) \bmod 77 \\
&= \left(\left[48^6 \bmod 77\right] \times \left[48^7 \bmod 77\right]\right) \bmod 77 \\
&= (15 \times 27) \bmod 77 \\
&= 405 \bmod 77 \\
&= 20. \\
M_2 &= R_2^{13} \bmod 77 \\
&= 58^{13} \bmod 77 \\
&= 58^{6+7} \bmod 77 \\
&= \left(58^6 \times 58^7\right) \bmod 77 \\
&= \left(\left[58^6 \bmod 77\right] \times \left[58^7 \bmod 77\right]\right) \bmod 77 \\
&= (36 \times 9) \bmod 77 \\
&= 324 \bmod 77 \\
&= 16.
\end{aligned}
$$

$$
\begin{aligned}
M_3 &= R_3^{13} \bmod 77 \\
&= 12^{13} \bmod 77 \\
&= 12^{6+7} \bmod 77 \\
&= \left(12^6 \times 12^7\right) \bmod 77 \\
&= \left(\left[12^6 \bmod 77\right] \times \left[12^7 \bmod 77\right]\right) \bmod 77 \\
&= (1 \times 12) \bmod 77 \\
&= 12 \bmod 77 \\
&= 12. \\
M_4 &= R_4^{13} \bmod 77 \\
&= 0^{13} \bmod 77 \\
&= 00 \\
M_5 &= R_5^{13} \bmod 77 \\
&= 5^{13} \bmod 77 \\
&= 5^{6+7} \bmod 77 \\
&= \left(5^6 \times 5^7\right) \bmod 77 \\
&= \left(\left[5^6 \bmod 77\right] \times \left[5^7 \bmod 77\right]\right) \bmod 77 \\
&= (71 \times 47) \bmod 77 \\
&= 3337 \bmod 77 \\
&= 26. \\
M_6 &= R_6^{13} \bmod 77 \\
&= 0^{13} \bmod 77 \\
&= 00. \\
M_7 &= R_7^{13} \bmod 77 \\
&= 12^{13} \bmod 77 \\
&= 12. \\
M_8 &= R_8^{13} \bmod 77 \\
&= 22^{13} \bmod 77 \\
&= 22^{6+7} \bmod 77 \\
&= \left(22^6 \times 22^7\right) \bmod 77 \\
&= \left(\left[22^6 \bmod 77\right] \times \left[22^7 \bmod 77\right]\right) \bmod 77 \\
&= (22 \times 22) \bmod 77 \\
&= 22 \bmod 77 \\
&= 22. \\
M_9 &= R_9^{13} \bmod 77 \\
&= 42^{13} \bmod 77 \\
&= 42^{6+7} \bmod 77 \\
&= \left(42^6 \times 42^7\right) \bmod 77
\end{aligned}
$$

$$
\begin{aligned}
&= \left(\left[42^6 \bmod 77\right] \times \left[42^7 \bmod 77\right]\right) \bmod 77 \\
&= (42 \times 70) \bmod 77 \\
&= 484 \bmod 77 \\
&= 14.
\end{aligned}
$$

$$
\begin{aligned}
M_{10} &= R_{10}^{13} \bmod 77 \\
&= 1^{13} \bmod 77 \\
&= 1 \bmod 77 \\
&= 01.
\end{aligned}
$$

Obtienes así el número del mensaje original

$$\mathscr{M} = 20161200260012221401.$$

P5: Finalmente, utilizando la tabla de asignaciones de números a las letras y espacio, convierte $\mathscr{M}$ a texto:

20	16	12	00	26	00	12	22	14	01
S	0	L		Y		L	U	N	A

Para terminar este ejemplo, veamos cómo el **receptor** determinó su clave pública y cómo calculó su número secreto s.

Recordemos que la construcción de la `clave pública` consiste de los siguientes pasos:

(a) Elige al azar dos números primos p y q y toma n como el producto de p y q:

$$n = pq.$$

En este caso, el **receptor** eligió $p = 7$ y $q = 11$; por tanto,

$$n = 77.$$

(b) A continuación, con el fin de definir r, el **receptor** calcula el mínimo común múltiplo de $p-1$ y $q-1$, al que llama m:

$$
\begin{aligned}
m &= \text{mcm}(p-1, q-11) \\
&= \text{mcm}(7-1, 11-1) \\
&= \text{mcm}(6, 10) \\
&= 30;
\end{aligned}
$$

Así,

$$m = 30.$$

(c) El número r es cualquier número entre 1 y m de manera que r y m sean primos entre sí, es decir, r será un número entre 1 y 30. En este caso, el **receptor** eligió $r = 7$, pues

$$1 < 7 < 30$$

y

$$\text{mcd}(7, 30) = 1.$$

Una vez que el **receptor** elaboró su clave pública, procedió a calcular su número secreto s; recuerda que este debe cumplir la propiedad

$$(rs) \bmod m = 1.$$

Para encontrarlo, el **receptor** calculó los números $r^2 \bmod m$, $r^3 \bmod m$, ...hasta que $r^t \bmod m = 1$:

$$\begin{aligned} r^2 \quad \text{mód } 30 &= 7^2 \bmod 30 \\ &= 49 \bmod 30 \\ &= 19 \\ r^3 \quad \text{mód } 30 &= 7^3 \bmod 30 \\ &= 13 \\ r^4 \quad \text{mód } 30 &= 7^4 \bmod 30 \\ &= 1. \end{aligned}$$

Esto significa que $t = 4$ y, por tanto,

$$\begin{aligned} s &= r^{t-1} \bmod m \\ &= 7^3 \bmod 30 \\ &= 13. \end{aligned}$$

En resumen, el número secreto del **receptor** es $s = 13$.

2. Supongamos que la clave que el receptor ha **publicado** es:

$$(77, 7)$$

y que ha recibido el siguiente mensaje cifrado:

$$\begin{aligned} &60012337600057371251476821006037105800 14 \\ &01603747001458480047535222124801680100 60 \\ &47120052016801372058003922470031011421 58 \\ &68003168475800520119010013584858216858 48 \end{aligned}$$

Vamos a descifrarlo. Para ello, apliquemos el protocolo RSA.

Lo primero que tenemos que hacer es calcular m y el número secreto s pero, dado que la clave pública es la misma que la del ejemplo anterior, ya sabemos que $m = 30$ y $s = 13$. Ahora, para descifrar el texto, recordemos que cada par de números representa una letra y que cada número del texto cifrado representamos con la letra R seguida de subíndices; así,

$$R_1 = 60, \quad R_2 = 01, \quad R_3 = 23, \quad R4 =, \ 37\ldots$$

Lo que vamos a calcular ahora son los números M_1, M_2, M_3, etcétera. Para ello, utilizaremos la fórmula

$$M_i = R_i^s \bmod n,$$

donde s es el número secreto y $n = 77$. Así, tenemos:

$$\begin{aligned} M_1 &= R_1^{13} \bmod 77 \\ &= 60^{13} \bmod 77 \\ &= 60^{6+7} \bmod 77 \\ &= \left(60^6 \times 60^7\right) \bmod 77 \\ &= \left(\left[60^6 \bmod 77\right] \times \left[60^7 \bmod 77\right]\right) \bmod 77 \\ &= (71 \times 25) \bmod 77 \\ &= 4. \end{aligned}$$

Por tanto, la letra que 60 representa es la D.

$$\begin{aligned} M_1 &= R_2^{13} \bmod 77 \\ &= 1^{13} \bmod 77 \\ &= 1^{6+7} \bmod 77 \\ &= \left(1^6 \times 1^7\right) \bmod 77 \\ &= \left(\left[1^6 \bmod 77\right] \times \left[1^7 \bmod 77\right]\right) \bmod 77 \\ &= (1 \times 1) \bmod 77 \\ &= 1. \end{aligned}$$

Luego, la letra que 01 representa es la A.

Si completamos los cálculos, obtendremos que el texto cifrado corresponde al siguiente texto:

DAVID HILBERT DIJO NADIE NOS EXPULSARA DEL PARAISO QUE CANTOR CREO PARA NOSOTROS

El método de Vigenère

Blaise de Vigenère fue un diplomático francés nacido en 1523. A la edad de 29 años, Vigenère estudió de Alberti, Trithemius y Porta, criptógrafos que habían desarrollado un método de codificación utilizando varios alfabetos. Aunque el método que vamos a explicar no es original del diplomático francés, sin ignorar las contribuciones de los tres hombres, Vigenère le llevó el método a su forma final, por lo que recibió su nombre y fue, hasta el siglo XIX, un método indescifrable.

Se atribuye a César, el primer emperador Romano, el siguiente procedimiento para codificar un mensaje:

Cada letra del mensaje original se sustituye por otra letra del alfabeto que está cuatro lugares adelante en el alfabeto.

En otras palabras, la letra "A" se sustituye por "D", la letra "B" por "E", etcétera. En el siguiente

cuadro se muestran todas las sustituciones de las 27 letras del alfabeto español:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Con esta técnica de cifrado, el mensaje

EL NÚMERO CERO SÍ ES UN NÚMERO NATURAL

se codifica de la siguiente manera:

HL PXOHUR FHUR VL HV PXOHUR PDWXUDÑ

(Hemos omitido las tildes). El alfabeto "desplazado" cuatro lugares hacia adelante será denominado *alfabeto de codificación*.

La idea general del cifrado de Vigenère es la de utilizar más de un alfabeto de codificación para codificar el texto. Por ejemplo, utilicemos tres:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O

La primera letra del mensaje, la "E" será codificada con el primer alfabeto, con la "H"; la segunda letra, la "L" se codificará con el segundo alfabeto, con la "Q"; la tercera letra, la "N", con el tercer alfabeto, con la "D". Así, las tres primeras letras del mensaje se codificará así:

HQ D

La cuarta letra, la "Ú", se codificará nuevamente con el primer alfabeto; la quinta letra con el segundo alfabeto, la sexta letra con el tercer alfabeto, la séptima letra con el primer alfabeto, y así hasta completar todas las letras del mensaje. Al final de este proceso, el mensaje quedará cifrado de la siguiente manera:

HQ DXRTUU RHXE VÑ TV AC PABHXE PGJXXPÑ

Como se puede observar, en esta nueva codificación, la segunda palabra "NÚMERO" se codifica de manera diferente que la primera vez.

Con la idea anterior, el método de Vigenère es el siguiente:

1. El **emisor** y el **receptor** eligen una *clave*, que consiste de una o varias palabras, y que solo ellos conocen.

2. El número de alfabetos de codificación que se utilizará es igual al número de letras que tiene la *clave*.

3. Los alfabetos se eligen de acuerdo a las letras de la *clave* y del denominado *cuadrado de Vigenère*:

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

Veamos un ejemplo

Ejemplo: Cifrado de Vigenère

1. El emisor establece que la *clave* es SMAP. Esto significa que la codificación va a utilizar los cuatro alfabetos que, en el cuadrado de Vigenère, empiezan con las letras "S", "M", "A" y "P":

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

Por tanto, se utilizarán los alfabetos de codificación números 19, 12, 27 y 16 –en este orden– para codificar cada letra del mensaje. Por ejemplo, el mensaje

EL NÚMERO CERO SÍ ES UN NÚMERO NATURAL

se codificará de la siguiente manera:

1. La primera letra, la "E" será codificada con el alfabeto número 19 (corresponden a la letra "S" de la *clave*); en este, la "E" se codifica con la letra "W".
2. La segunda letra del mensaje, la "L", se codificará con el alfabeto 12; en este, la "L" es reemplazada por la letra "W".
3. La tercera letra del mensaje, la "N", se codifica con el alfabeto 27; así, esta letra no se sustituye con ninguna letra porque es el mismo alfabeto original.
4. La cuarta letra, la "U", se codifica con el alfabeto 16; así, esta letra se sustituye por la letra "K".
5. Para la quinta letra, se utiliza nuevamente el alfabeto 19; así, "M" es reemplazada por "E".
6. La sexta letra "E" es reemplazada por "P", pues se utiliza el alfabeto 12.
7. La séptima letra "R" no se sustituye con otra letra porque se utiliza el alfabeto 27.
8. La octava letra "O" es sustituida por la letra "E", porque se usa el alfabeto 16.

Por tanto, del texto

EL NÚMERO

es codificada por

WW NKEPRE.

Luego de aplicar el método al mensaje original, se obtiene el mensaje codificado:

WW NKEPRE UPRE LT EI NY NKEPRE FMTKKML

2. Si la *clave* es SOL, el mensaje cifrado

WZ NWGZ WH ASG

se obtuvo mediante tres alfabetos: 19, 15 y 11, que son los que corresponden a las letras "S", "O" y "L", respectivamente. Por tanto, cada letra del mensaje cifrado proviene de codificar el mensaje original con los alfabetos 19, 15, 11, 19, 15, 11, etcétera:

W	Z	N	W	G	Z	W	H	A	S	G
19	15	11	19	15	11	19	15	11	19	15
E	L	C	E	R	O	E	S	P	A	R

Es decir, el mensaje original es:

EL CERO ES PAR

El método Hill

Supongamos que el objetivo es encriptar el mensaje

'BIENVENIDOS AL TORNEO DE CIENCIAS'

en un grupo de palabras que sea ilegible para alguien que no conozca la clave secreta.

Para aplicar este método, primero una clave, que la presentaremos como una matriz cuadrada de orden 2; a esta matriz le nombraremos con la letra C.

Como ejemplo, supongamos que

$$C = \begin{bmatrix} 3 & -5 \\ 4 & -7 \end{bmatrix}.$$

Procedemos de la siguiente manera:

- **Primer paso:** Contamos la cantidad de letras *y espacios* en el mensaje. Si la cantidad es impar, le debemos aumentar un espacio al final. El mensaje

  BIENVENIDOS AL TORNEO DE CIENCIAS

  tiene 33 letras y espacios. Por lo tanto, debemos aumentarle un espacio al final:

  'BIENVENIDOS AL TORNEO DE CIENCIAS_

- **Segundo paso:** Obtenemos un nuevo texto al sustituir cada letra mayúscula y espacio por un número de dos cifras. Los números que utilizaremos son los siguientes:

Letra	Número	Letra	Número	Letra	Número	Letra	Número
' '	00	A	01	B	02	C	03
D	04	E	05	F	06	G	07
H	08	I	09	J	10	K	11
L	12	M	13	N	14	Ñ	15
O	16	P	17	Q	18	R	19
S	20	T	21	U	22	V	23
W	24	X	25	Y	26	Z	27

A los espacios en blanco, les corresponde el número 00. De esta forma, el texto

'BIENVENIDOS AL TORNEO DE CIENCIAS'

se codifica por

02090514230514090416200001120021161914051600040500030905140309012000

- **Tercer paso:** Encriptaremos el código anterior: agrupamos a este en grupos de 4 cifras consecutivas. Cada par de cuatro cifras cada uno, le consideramos como una fila de una matriz cuadrada de orden 2; cada una de estas filas, se deberán multiplicar por la matriz clave C. A cada número de la fila obtenida, le aplicamos la operación módulo 28l resultado le aplicamos la operación mód 28. Por ejemplo, para las primeras cuatro cifras, hacemos el siguiente proceso:

$$\underbrace{0209}_{(02\ 09)}05142305140904162000011200211619140516000405000309051403090120$$

Multiplicamos la fila (02 09) por la matriz clave C:

$$\begin{aligned}(02 \quad 09)C &= (02 \quad 09)\begin{pmatrix} 3 & -5 \\ 4 & -7 \end{pmatrix} \\ &= ((02)(3)+(09)(4) \quad (02)(-5)+(09)(-7)) \\ &= (42 \quad -73).\end{aligned}$$

Finalmente, a cada número de esta fila le aplicamos la operación mod 28:

$$42 \bmod 28 = 14 \quad \text{y} \quad -73 \bmod 28 = 11.$$

Obtenemos, entonces, la fila

$$(14 \quad 11).$$

Repetimos este proceso con cada grupo de cuatro cifras, y obtenemos:

Código original	Código encriptado	Código original	Código encriptado
0209	1411	0514	1517
2305	0518	1409	2207
0416	2008	2000	0412
0112	2323	0021	0021
1619	1211	1405	0607
1600	2004	0405	0401
0003	1207	0905	1904
1403	2621	0901	0304
2000	0412		

Y texto encriptado es:

14111517051822072008041223230021121106072004040112071904262103040412

Cuarto paso: Cada par consecutivo de números es "decodificado" a letras. Obtenemos:

NKÑPEQUGSHDLVV TLKFGSDDALGRDYTCDDL

De esta forma, el mensaje original

'BIENVENIDOS AL TORNEO DE CIENCIAS'

se encripta en

NKÑPEQUGSHDLVV TLKFGSDDALGRDYTCDDL

Decodificación: recuperación del texto original

Para poder recuperar el mensaje original, utilizaremos la matriz inversa de la matriz clave C.

Descubramos el texto encriptado por

AMKBKWCO

Supongamos que el texto original fue encriptado con la clave C:

$$C = \begin{pmatrix} 3 & -5 \\ 4 & -7 \end{pmatrix}$$

Esta información es muy importante. Gracias a que tenemos la clave C, seremos capaces de descifrar el mensaje original. Pero, para esto, necesitaremos encontrar la matriz inversa.

Para encontrar la inversa, calculemos el determinante de C:

$$|C| = (3)(-7) - (4)(-5) = -1.$$

Por tanto:

$$C^{-1} = \begin{pmatrix} \frac{-7}{-1} & \frac{5}{-1} \\ \frac{-4}{-1} & \frac{3}{-1} \end{pmatrix} = \begin{pmatrix} 7 & -5 \\ 4 & -3 \end{pmatrix}.$$

Procedamos a la decodificación:

- **Primer paso:** Hallamos el módulo en base 28 de cada elemento de la matriz inversa. En este caso, tenemos que

  $$7 \bmod 28 = 7, \quad -5 \bmod 28 = 23, \quad 4 \bmod 28 = 4 \quad \text{y} \quad -3 \bmod 28 = 25.$$

  Definamos la matriz C^* cuyas filas son los módulos 28 de los elementos de C:

  $$C^* = \begin{pmatrix} 7 & 23 \\ 4 & 25 \end{pmatrix}.$$

- **Segundo paso:** Codificamos cada letra el mensaje encriptado a números: de

  AMKBKWCO

  se obtiene:

  0113110211240316

- **Tercer paso:** En este paso, recuperaremos el código original. Para ello, la cadena de números obtenidos le organizamos en grupos 4 cifras consecutivas

  $$\underbrace{0113}_{(01\ 13)}110211240316$$

  Con cada un de los pares, formamos una fila de una matriz cuadrada, la que multiplicamos por la matriz C^*, y luego aplicamos la operación $\bmod 28$. Por ejemplo:

  $$\begin{aligned} (01\ 13)C^* &= (01\ 13)\begin{pmatrix} 7 & 23 \\ 4 & 25 \end{pmatrix} \\ &= ((01)(7)+(13)(4), (01)(23)+(13)(25)) \\ &= (59\ 348) \end{aligned}$$

  A cada número de esta fila le aplicamos $\bmod 28$:

  $$59 \bmod 28 = 03 \quad \text{y} \quad 348 \bmod 28 = 12;$$

  de forma que obtenemos la fila

  $$(03\ 12).$$

  Repetimos este proceso con las siguientes cuatro cifras; obtenemos:

Código encriptado	Código original	Código encriptado	Código original
0113	0312	1102	0123
1124	0513	0316	0121

El código original de corrido es

0312012305130121

- **Cuarto paso:** Cada par de cifras se decodifican en letras del alfabeto:

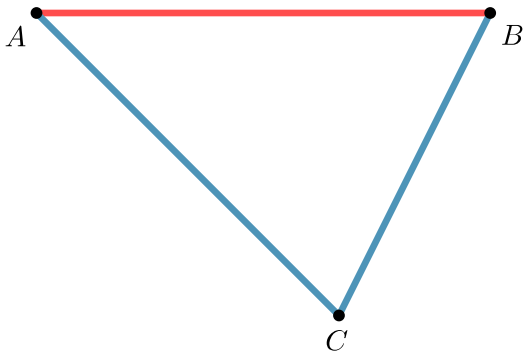
  CLAVEMAT

  como se puede observar si se mira la tabla de letras-números.

Triangulación

La **triangulación** es un procedimiento que permite obtener la distancia entre dos puntos sin la necesidad de una medición directa. De modo general, si se requiere conocer la distancia que separa dos puntos A y B entre sí:

Triangular significa encontrar un tercer punto C, de forma que se puedan conocer de algún modo las distancias de C a A o de C a B, o los ángulos $\angle CAB$ $\angle CBA$. Con esa información y algunas relaciones trigonométricas sencillas, se podrá obtener de manera bastante precisa la distancia entre A y B.



Veamos algunos casos comunes.

1. Supongamos que entre A y B hay una quebrada, razón por la cual no es posible medir la distancia entre estos puntos directamente. Si se localiza un punto C de manera que se puedan conocer las distancia AC y BC (por ejemplo, midiéndolas directamente, o porque ya son conocidas) y la medida del ángulo $\angle ACB$, la *ley de los cosenos* nos permitirá obtener fácilmente AB.

   A manera de ejemplo, si la distancia AC es 90 metros, BC es 100 metros y la medida del ángulo ACB es 30 grados, entonces por la ley de los cosenos, tenemos que

   $$AB^2 = AC^2 + BC^2 - 2AC \cdot BC \cos \angle C$$

$$
\begin{aligned}
&= 90^2 + 100^2 - 2(90)(100)\cos 30^\circ \\
&= 8\,100 + 10\,000 - 18\,000\cos 30^\circ \\
&= 18\,100 - 1800\frac{\sqrt{3}}{2} \\
&\approx 2\,511.54.;
\end{aligned}
$$

por tanto,

$$AB \approx \sqrt{2,511.54} \approx 50.12.$$

Es decir, la distancia entre los puntos A y B es aproximadamente 50.12 metros.

2. Ahora supongamos que solo conocemos la distancia AC y los ángulos $\angle CAB$ y $\angle CBA$. En este caso, la *ley de senos* nos viene a auxiliar para conocer la distancia AB.

   Como ejemplo, supongamos que AC es igual a 90 metros, el ángulo $\angle ABC$ mide 63.89 grados y el ángulos $\angle BAC$ mide 86.11 grados. Entonces, por la ley de senos tenemos que:

$$
\begin{aligned}
\frac{AC}{\operatorname{sen}\angle B} = \frac{BC}{\operatorname{sen}\angle A} &\equiv \frac{90}{\operatorname{sen} 63.89} = \frac{BC}{\operatorname{sen} 86.11} \\
&\equiv \frac{90}{0.8980} \approx \frac{BC}{0.9977} \\
&\equiv 100.23 \approx \frac{BC}{0.9977},
\end{aligned}
$$

   de donde obtenemos que

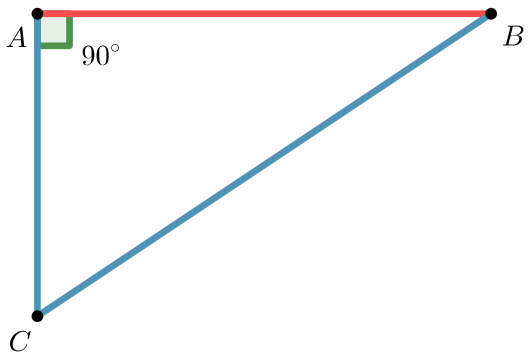
$$BC \approx 0.9977 \times 100.23 \approx 100$$

   metros. Y, ahora utilizamos la ley de cosenos, como en el ejemplo anterior, ya que ahora conocemos los lados AC y BC y también el ángulo C, ya que la suma de las medidas de los tres ángulos es igual a 180:

$$86.11 + 63.89 + \mathrm{m}\angle C = 180,$$

   de donde $\mathrm{m}\angle C = 30$.

3. Imaginemos que el punto C se elige de manera que el ángulo BAC es recto:



   En este caso, el teorema de Pitágoras o las definiciones de *seno*, *coseno* o *tangente* nos dan la solución imediatamente.

   Por ejemplo, en el primer ejemplo, si $AC = 90$ y $BC = 100$, entonces por el teorema de

Pitágoras, tenemos que

$$BC^2 = AC^2 + AB^2$$
$$100^2 = 90^2 + AB^2$$
$$10\,000 = 8\,100 + AB^2,$$

de donde

$$AB^2 = 1\,900;$$

es decir,

$$AB = \sqrt{1\,900} \approx 43.59$$

metros.

O si sabemos que $AC = 90$ y que $\angle C$ mide 30 grados, entonces

$$\tan \angle C = \frac{AB}{AC}$$
$$\tan 30 = \frac{AB}{90}$$
$$0.5774 \approx \frac{AB}{90},$$

de donde

$$AB \approx 0.5774 \times 90 \approx 51.96$$

metros.