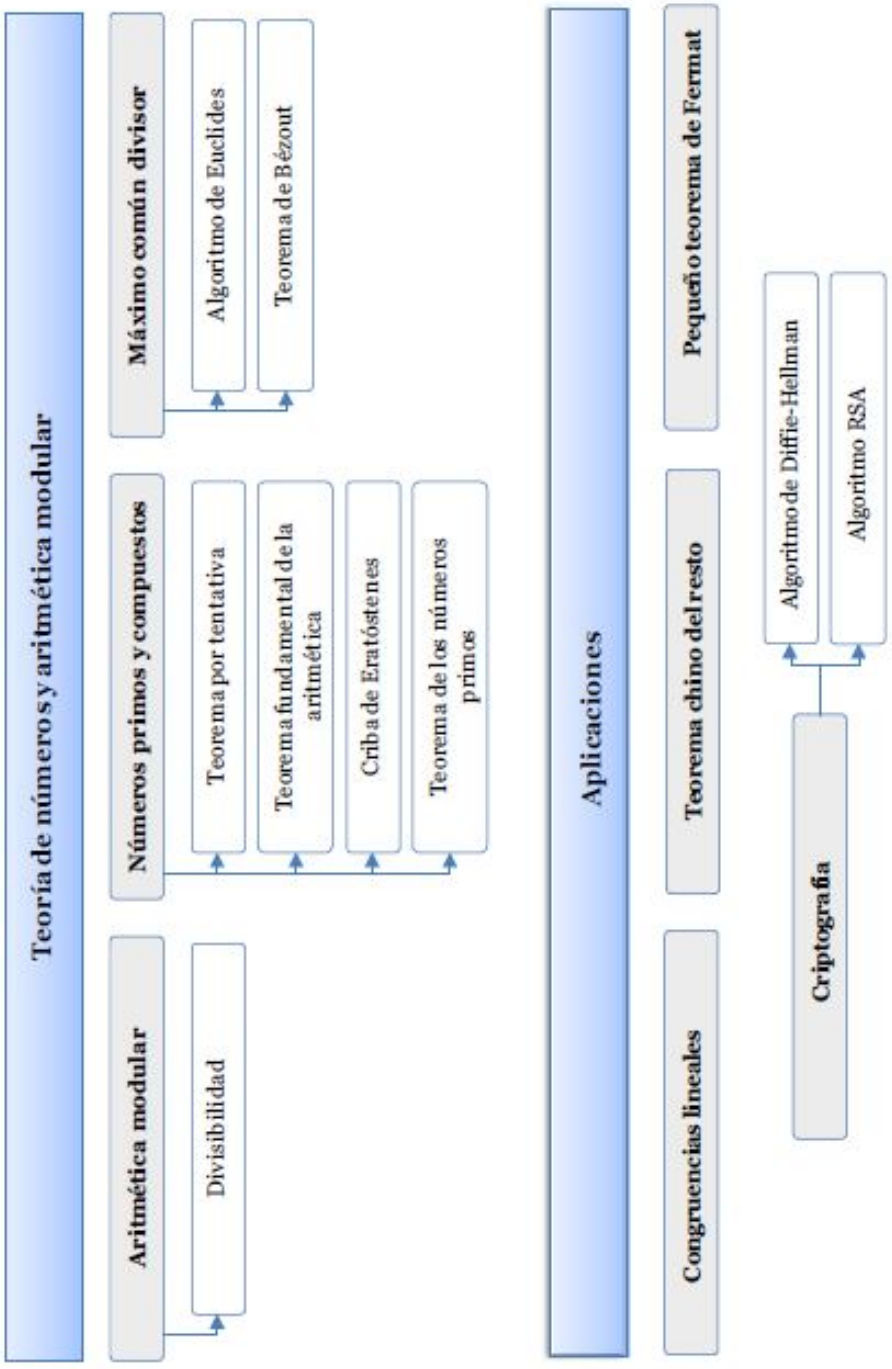
Tema 6

Álgebra y Matemática discreta

Teoría de números y aritmética modular. Aplicaciones

Índice

Esquema


Teoría de números y aritmética modular
Aritmética modular
Divisibilidad
Números primos y compuestos
Teorema por tentativa
Teorema fundamental de la aritmética
Criba de Eratóstenes
Teorema de los números primos
Máximo común divisor
Algoritmo de Euclides
Teorema de Bézout
Aplicaciones
Congruencias lineales
Teorema chino del resto
Criptografía
Algoritmo de Diffie-Hellman
Algoritmo RSA
Pequeño teorema de Fermat

Ideas clave

6.1 Introducción y objetivos

La teoría de números es una rama de las matemáticas que se centra en el estudio de los números y sus propiedades. Desde la antigüedad, ha sido un área fascinante e importante de las matemáticas, y ha desempeñado un papel fundamental en el desarrollo de la ciencia y la tecnología.

En este tema, estudiaremos la aritmética modular, una parte de la teoría de números, que se presenta como una herramienta poderosa para analizar las propiedades de los números enteros. La aritmética modular se basa en la idea de que dos números enteros son equivalentes si al ser divididos por un número fijo (llamado módulo) dan el mismo residuo. Esta idea de equivalencia es útil para estudiar propiedades como , los números primos, las congruencias o la divisibilidad, siendo este, como veremos a lo largo del tema, un concepto fundamental en la teoría de números, que se refiere a la capacidad de un número para ser dividido exactamente por otro. Por ejemplo, el número 15 es divisible por 3 y por 5, pero no es divisible por 7. Esto, nos lleva a la definición de los números primos, como aquellos que solamente son divisibles por sí mismos y por la unidad, que nos sirve para introducir una idea principal en la teoría de números como es la de máximo común divisor y el mínimo común múltiplo, fundamental en la teoría de números y en la aritmética. Ambos son herramientas útiles para resolver problemas de divisibilidad y factorización de números enteros.

Como veremos a lo largo del tema, el máximo común divisor (MCD) es el número más grande que divide exactamente a dos o más números enteros. Por ejemplo, el MCD de 12 y 18 es 6, ya que 6 es el mayor número que divide exactamente a ambos números. El MCD también se puede calcular mediante el algoritmo de Euclides, que consiste en

dividir repetidamente el número más grande entre el más pequeño y tomar el residuo hasta que se llegue a un residuo de cero.

Por otro lado, el mínimo común múltiplo (mcm) es el número más pequeño que es múltiplo común de dos o más números enteros. Por ejemplo, el mcm de 4 y 6 es 12, ya que 12 es el menor número que es múltiplo tanto de 4 como de 6. Tanto el MCD como el mcm tienen muchas aplicaciones prácticas, como en el diseño de algoritmos, la resolución de problemas de fracciones y la optimización de tiempos y recursos. Por ejemplo, en la programación de computadoras, se utilizan con frecuencia para simplificar fracciones y evitar errores de redondeo.

Además, la aritmética modular, permite dar respuesta a aplicaciones prácticas y problemas matemáticos en los cuales únicamente se está interesado en calcular u obtener el resto de la división de dos enteros, incluyendo la criptografía, la codificación de mensajes, la teoría de números o la informática. Algunas de las aplicaciones más importantes de la aritmética modular, tal como veremos a lo largo del tema son:

Teorema chino del resto, que establece que, dado un sistema de congruencias lineales, es posible encontrar una solución única que satisface todas las congruencias simultáneamente. Este teorema es muy útil en la teoría de números y en la informática, donde se utiliza para dividir grandes problemas en subproblemas más pequeños.

La criptografía que tiene como objetivo proteger información confidencial. Uno de los ejemplos más famosos es el algoritmo RSA, que utiliza la aritmética modular para encriptar y desencriptar mensajes. También en la teoría de números, como se ha visto, la aritmética modular es fundamental, donde se utiliza para estudiar las propiedades de los números enteros y los números primos. Por ejemplo, el teorema chino del resto, que es un resultado importante de la aritmética modular, se utiliza para resolver ecuaciones diofánticas.
Aprenderemos por tanto, en este tema, cómo resolver congruencias lineales haciéndonos valer del pequeño teorema de Fermat, sistemas de congruencias lineales mediante el teorema chino del resto y otro tipo de ecuaciones no lineales haciéndonos

valer del concepto de logaritmo discreto. Manejar estas operaciones resulta esencial para comprender muchos sistemas criptográficos, los cuales utilizan teoría de números como herramienta fundamental a fin de mejorar la ciberseguridad.

En este tema se pretende , alcanzar los siguientes objetivos:

- Conocer las nociones en las que se construye la teoría de números.
- Obtener la descomposición en factores primos de un número entero positivo.
- Manejar el teorema de la división euclídea y utilizarlo para desarrollar el algoritmo de Euclides.
- Hallar el máximo común divisor y mínimo común múltiplo de dos números enteros.
- Manejar con soltura las operaciones suma y producto en los conjuntos finitos $\mathbb{Z}_m$ con $m \in \mathbb{R}$
- Emplear adecuadamente el Pequeño Teorema de Fermat y el teorema chino del resto para resolver congruencias y sistemas de congruencias lineales.
- Comprender el concepto de raíz primitiva y logaritmo discreto y aplicarlo para resolver congruencias no-lineales sencillas.
- Conocer algoritmos: RSA y Diffie-Hellman.

Para alcanzar estos objetivos, se propone la siguiente subdivisión del contenido de este tema:

- Divisibilidad y aritmética modular.
- Números primos.
- Máximo común divisor y mínimos común múltiplo.
- Congruencias lineales.

- Teorema chino del resto
- Pequeño teorema de Fermat.
- Algoritmo de Diffie-Hellman.
- Algoritmo RSA.

6.2 Divisibilidad y aritmética modular

Comenzamos esta sección aclarando que cuando hablamos de teoría de números, nos estamos refiriendo a la rama de la matemática que estudia las propiedades de los números enteros y su divisibilidad, mientras que la aritmética modular estudia las operaciones y propiedades de *congruencia* entre enteros, respecto a un *módulo* y definimos el concepto de divisibilidad de la siguiente manera:

Definición 1

Sean a y d números enteros, decimos que d ***divide*** a a y lo notamos como $d|a$, si existe un entero q tal que $a = dq$. En este caso también decimos que a ***es múltiplo de*** d. Por convención todo entero divide a cero.

Ejemplo 1.

Determinar si $3|7$ y si $3|12$.

Solución:

- Se tiene que $3 \not| 7$, ya que no existe ningún número q que cumpla que $7 = 3 \cdot q$
- Por otro lado, $3|12$ ya que podemos escribir $12 = 4 \cdot 3$

Por tanto, decir que a es múltiplo de d es equivalente a decir que d es divisible entre a. Por homogeneidad, la relación $d|a$ la leeremos como d divide a a, o como a es múltiplo de d. En caso de que a no sea dividido por d, lo representamos como $d \not| a$

Teorema 1

Sean a, b y c tres números enteros, entonces se pueden demostrar las siguientes propiedades de la divisibilidad:

- si $a|b$ y $a|c$, entonces $a|(b + c)$

- si $a|b$, entonces $a|bc$ para todo entero c
- si $a|b$ y $b|c$, entonces $a|c$

Y se generalizan estas propiedades en el siguiente corolario:

Corolario 1

Si a, b y c son números enteros en los que se cumple que $a|b$ y $a|c$, entonces, $a|mb + nc$ siendo m y n números enteros cualesquiera.

Si $d|a$, el teorema de la división afirma que $a = dq + r$, siendo q y r números enteros únicos, tañes que $0 \leq r < d$. Y además, llamaremos a d **divisor** de a, a q, **cociente** de a y a r lo llamamos **resto**. Denotamos por q a la división entera de a, es decir $q = a|d$ mientras que al resto de la división, r, lo denotamos como $r = a \; mod \; d$, que se lee r igual a a módulo d. En otras palabras, si a es dividido entre d y esa división no es exacta, el residuo de esta es denotado como $r = a \; mod \; d$".

Por ejemplo, si tenemos $r = 13 \; modulo \; 5$, esto significa que r es el residuo de la división de 13 entre 5, es decir, $r = 3$, ya que 13 dividido por 5 es 2 con un residuo de 3. Por lo tanto, 13 módulo 5 es igual a 3.
Si tomamos $m = 2$, podemos escribir:

- Para $a = 5, \;\; a = 2 \cdot 2 + 1$
- Para $a = 6, \;\; a = 3 \cdot 2 + 0$
- Para $a = 7, \;\; a = 3 \cdot 2 + 1$
- Para $a = 8, \;\; a = 4 \cdot 2 + 0$

Así, para un m determinado, podemos clasificar todos los a según su resto r.
Sean a, b enteros y m un entero positivo, decimos que a es **congruente** con b en módulo m si $m|(a - b)$. Equivalentemente, a se puede escribir como b más un múltiplo de m : $a = b + mk$, con k entero. En este caso denotamos $a \equiv b(mod \; m)$. De esta forma, siguiendo el ejemplo anterior, escribimos $5 \equiv 7(mod 2)$, es decir, 5 y 7 tienen el mismo resto al dividir entre 2. 5 y 7 son congruentes *módulo 2*.

La relación que acabamos de definir entre a y b es un caso particular de relación de equivalencia y en ella se cumplen las siguientes propiedades:

Definición 2

En una relación de congruencia, se pueden demostrar las siguientes propiedades:

- **Reflexiva:** $a \equiv a \text{ mod}(m)$
- **Simétrica:** Si $a \equiv b \text{ mod}(m)$, entonces $b \equiv a \text{mod}(m)$
- **Transitiva:** Si $a \equiv b \text{ mod } (m)$ y $b \equiv c \text{mod } (m)$, entonces, $a \equiv c \text{ mod}(m)$

Se llama **clase de congruencia** de a en módulo m al conjunto de todos los enteros congruentes con a en módulo m. Así, dado un módulo m, definimos $\mathbb{Z}_m$ como el conjunto de números enteros no negativos menores que m, como los representantes canónicos de cada clase, es decir:

$$\mathbb{Z}_m = \{0, 1, 2, ..., m-1\}$$

En definitiva, las clases de equivalencia, no es más que la formalización de "agrupar los números según el resto r". Así, continuando con el ejemplo anterior, para el módulo 2, tenemos unicamente como restos el 0 y el 1 y en tal caso, hablaremos de la clase del 0 en módulo 2 y la clase del 1 en módulo 2. Podemos por tanto decir que el 5 y el 7 pertenecen a la clase del 1 en $\mathbb{Z}_2$. Generalizando,decimos que la clase de 0 son todos los números pares mientras que la clase del 1 son todos los números impares para $\mathbb{Z}_2$. Nótese entonces, que podemos escribir $[16]_2 = [8]_2 = [0]_2$.

Ejemplo 2.

Vamos a analizar las clases en $\mathbb{Z}_5$:

- Para la relación $a = 5 \cdot q + r$, encontramos que r solo puede tomar los valores $0, 1, 2, 3, 4$, ya que si r=5, el resto será 0.
- Podemos escribir $73 = 70 + 3 = 14 \cdot 5 + 3$, es decir, $73 \in [3]_5$

- Las clases canónicas del 5 son:
  - $[0]_5 = 0 + 5 \cdot k, \ \ k \in \mathbb{Z}$
  - $[1]_5 = 1 + 5 \cdot k, \ \ k \in \mathbb{Z}$
  - $[2]_5 = 2 + 5 \cdot k, \ \ k \in \mathbb{Z}$
  - $[3]_5 = 3 + 5 \cdot k, \ \ k \in \mathbb{Z}$
  - $[4]_5 = 4 + 5 \cdot k, \ \ k \in \mathbb{Z}$

Para las relaciones de congruencia, se pueden definir las operaciones suma y producto, y así se engloba en la aritmética modular en $\mathbb{Z}_m$ al resultado de las operaciones aritméticas que realizamos en módulo m.

6.3 Aritmética modular

Aunque la aritmética modular es un tema amplio, en este curso unicamente vamos a tratar la operación suma y producto de forma sencilla:

Definición 3

Sea m un número positivo cualquiera y sean a y b dos números congruentes en mod(m). Se define:

- La operación suma como: $[a]_m + [b]_m = [a+b]_m$
- La operación producto como: $[a]_m \cdot [b]_m = [a \cdot b]_m$

Veamos algunos ejemplos de sumas y productos en aritmética modular:

$$[2]_4 + [5]_4 = [2+5]_4 = [3]_4$$
$$[4]_5 + [4]_5 = [4+4]_5 = [3]_5;$$
$$[88]_5 + [4]_5 = [91]_5 = [4]_5$$

$$[10]_5 \cdot [2]_5 = [20]_5 = [0]_5$$
$$[4]_6 \cdot [5]_6 = [20]_6 = [2]_6$$

6.4 Números primos

Dado un número entero a, se denominan factores a los números enteros que dividen a a.

Definición 4

Un **número primo** p es un entero, cuyos únicos factores son $1, -1, p$ y $-p$. Por convenio se asume que $0, 1, -1$ no son números primos. Por otro lado, un número entero positivo mayor que 1 que no es primo, se denomina *compuesto*, es decir un número entero c que tiene más factores que $1, -1, p, -p$.

Ejemplo 3.

El entero 7 es primo, puesto que sus factores positivos son solamente 1 y 7, mientras que el entero 9 es compuesto, ya que es divisible por 3.

En este ejemplo es fácil ver que el 7 es número primo, pero para números mayores, resulta necesario encontrar algún procedimiento que nos permita discernir si un número es primo o no lo es. Para ello, tenemos dos resultados interesantes que nos permiten conocer el carácter de un número. Por ejemplo, tenemos el algoritmo de la *división por tentativa* o la *criba de Erastóstenes*. La división por tentativa es un algoritmo sencillo para determinar eficientemente si un número a es primo y consiste en intentar dividir a entre todo número primo menor o igual a $\sqrt{n}$. Si se encuentra un número que es divisor de a, ese número es un factor de a. Veamos cómo aplicar este método en el siguiente ejemplo.

Ejemplo 4.

Para ver si 749 es o no un número primo aplicando la división por tentativa, probamos con los números primos menores a $\sqrt{749} \approx 27.36$. Realizamos los cocientes:

$$\frac{749}{2}; \frac{749}{3}; \frac{749}{5}; \frac{749}{7}; \frac{749}{11}; \frac{749}{13}; \frac{749}{17}; \frac{749}{23}$$

y comprobamos que $7|749$ ya que $749 = 7{\cdot}107$ $(749/7 = 107)$.

Por otro lado, la criba de Eratóstenes es un algoritmo que permite encontrar todos los números primos positivos que no exceden un determinado valor n. Para llevarlo a cabo, se forma una tabla con todos los números naturales comprendidos entre 2 y n y se van tachando los números que son primos de la siguiente manera: comenzando por el 2, se tachan todos sus múltiplos; cuando se encuentra un número entero que no ha sido tachado, ese número es declarado primo y se procede a tachar todos sus múltiplos, así sucesivamente. El proceso termina cuando el cuadrado del siguiente número confirmado como primo es mayor que n. Se puede ver en la siguiente tabla de números naturales del 1 al 100, donde los números primos están señalizados color rojo.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~53~~	~~54~~	~~55~~	~~56~~	~~57~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

La importancia que toman los números primos en las matemáticas en general y concretamente en la teoría de números, viene dada por el **teorema fundamental de la aritmética**, que establece que cualquier número entero positivo mayor que 1 se puede expresar de manera única como un producto de números primos. En otras palabras, cualquier número entero positivo mayor que 1 puede escribirse como la multiplicación de un conjunto único de números primos en un orden específico.

Teorema 2

Teorema fundamental de la aritmética:

Todo número entero positivo mayor que 1 puede ser expresado de forma única (salvo por el orden de los factores) como un producto de factores primos.

Es decir, dado a un número entero, existen números primos positivos $p_1, p_2, ..., p_k$ y números naturales $r_1, r_2, ..., r_k$ de modo que

$$a = p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_k^{r_k} \; si \; a < 0$$

ó

$$a = -p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_k^{r_k} \; \; si \; a < 0$$

Por ejemplo, el número 24 se puede expresar como $2 \times 2 \times 2 \times 3$, y esta es la única forma de descomponer 24 como producto de números primos. No se puede escribir

como un producto de otros números primos distintos de 2 y 3. Este teorema es importante porque proporciona una forma sistemática de descomponer números en sus componentes primos (descomposición factorial). Esencialmente, nos dice que todos los números enteros positivos se construyen a partir de bloques fundamentales, los números primos, y que no hay nada más allá de estos bloques fundamentales. Por lo tanto, el teorema es una piedra angular de la teoría de números y tiene aplicaciones en muchos campos, incluyendo la criptografía y la informática teórica

Así, podemos utilizar la división por tentativa de forma sucesiva para encontrar la descomposición factorial de un número. Por ejemplo, este procedimiento para encontrar la descomposición factorial del número 10672, proporcionaría el siguiente resultado:

$$\frac{10672}{2} = 5336,\ \frac{5336}{2} = 2668,\ \frac{2668}{2} = 1334,\ \frac{1334}{2} = 667,\ \frac{667}{23} = 29,\ \frac{29}{29} = 1$$

Así, la descomposición en factores primos será: $10672 = 2^4 \cdot 23 \cdot 29$

Por otra parte, el **teorema de los números primos** indica que la probabilidad de que un número n elegido al azar sea primo no es mayor a $\frac{1}{ln(n)}$. Este resultado nos da una descripción general de cómo están distribuidos los números primos en el conjunto de los números naturales, lo que formaliza la idea intuitiva de que los primos son menos comunes cuanto más grandes son.

Definición 5

Dos números a, b son primos relativos si $m.c.d.(a, b) = 1$. Análogamente, los enteros $n_1, n_2, ..., n_k$ son primos por pares si siempre que $i \neq j$ se cumple que $m.c.d.(n_i, n_j) = 1$.

6.5 Máximo común divisor y mínimo común múltiplo

El Máximo Común Divisor (MCD) y el Mínimo Común Múltiplo (mcm) son dos conceptos importantes en la teoría de números y se utilizan frecuentemente en la resolución de problemas de matemáticas y en la simplificación de fracciones.

Definición 6

Dados a y b enteros, se llama máximo común divisor (m.c.d) al número entero positivo más grande d que cumple $d|a$ y $d|b$. Es decir, d es el máximo común divisor de a y b si:

$$d|a,\ d|b \text{ y además, si } c|a \text{ y } c|b, \text{ entonces } c \leq d.$$

Por consistencia, se define el $m.c.d.(0,n) = n$ 7 $m.c.d.(0,0) = 0$. Por tanto, el *máximo común divisor* es el mayor número entero que divide a dos o más números enteros sin dejar residuo. Por ejemplo, el $m.c.d$ de 12 y 18 es 6, porque 6 es el mayor número que divide exactamente a 12 y a 18.

El *mínimo común múltiplo* es el menor número entero que es múltiplo de dos o más números enteros. En otras palabras, es el número más pequeño que es divisible por todos los números en cuestión. Por ejemplo, el mcm de 12 y 18 es 36, porque 36 es el menor número que es divisible tanto por 12 como por 18.

Definición 7

El mínimo común múltiplo (m.c.m) de los enteros a, b es el entero positivo más pequeño m que es múltiplo de a y b, es decir $a|m$ y $b|m$. Es decir, m es el mínimo común múltiplo de a y b si:

$a|m,\ b|m$ y además, si $a|c$ y $b|c$, entonces $m \leq c$.

El teorema fundamental de la aritmética asegura que si a, b son números enteros, cada uno de ellos posee una factorización en números primos única proporciona un procedimiento para hallar el máximo común divisor y el mínimo común múltiplo de los números a y b:

$$m.c.d.(a,b) = p_1^{min\{r_1,s_1\}} \cdot p_2^{min\{r_2,s_2\}} \cdot \ldots \cdot_k^{min\{r_k,s_k\}}$$

$$m.c.d.(a,b) = p_1^{max\{r_1,s_1\}} \cdot p_2^{max\{r_2,s_2\}} \cdot \ldots \cdot_k^{max\{r_k,s_k\}}$$

Este método es exactamente el que aprendimos en la etapa de educación secundaria. Tal y como veremos en la siguiente sección, el Algoritmo de Euclides proporciona un método más eficiente que este para el cálculo del máximo común divisor.

Ejemplo 5.

Obtener la factorización en números primos de los números 10672 y 4147 y utilizarla convenientemente para hallar:

a) $d = m.c.d.(10672, 4147)$

b) $m = m.c.m.(10672, 4147)$.

Solución:

Tal y como hemos visto anteriormente, $10672 = 24{\cdot}23{\cdot}29$. Procediendo de forma análoga, se tiene que $4147 = 11{\cdot}13{\cdot}29$.

- Para hallar el máximo común divisor, tomamos los factores comunes al mínimo exponente: $m.c.d, (10672, 4147) = 29$.
- Para hallar el mínimo común múltiplo, tomamos los factores comunes y no comunes al máximo exponente: $m.c.m.(10672, 4147) = 2^4{\cdot}11{\cdot}13{\cdot}23{\cdot}29 = 1526096$.

Terminamos esta sección con un corolario que resulta de aplicación en diversas ramas de la matemática como, como la teoría de números, la teoría de grupos o la criptografía.

Corolario 2

Si a, b son números naturales mayores que 1, se cumple:

$$a \cdot b = m.c.d.(a, b) \cdot m.c.m.(a, b)$$

6.6 Algoritmo de Euclides e identidad de Bézout

Dos conceptos muy importantes en la teoría de números son el algoritmo de Euclides y el lema de Bezout. mediante el algoritmo de Euclides, podemos encontrar el máximo común divisor (MCD) de dos números enteros. Se basa en la observación de que si a y b son dos números enteros, y a es mayor que b, con $b > 0$, entonces existen enteros q y r tales que:

$$a = bq + r \ \ con \ \ 0 < |r| < \ b.$$

El lema de Bezout es una consecuencia del algoritmo de Euclides, y establece que para dos números enteros a y b, existe otro par de números s, t (denominados coeficientes de Bezout) tales que:

$$as + bt = m.c.d.(a, b)$$

Esta ecuación se conoce como *identidad de Bezout* y puede ser encontrada utilizando el algoritmo de Euclides y trabajando hacia atrás en las ecuaciones que se van generando durante el proceso. El lema de Bezout es importante porque nos dice que cualquier par de números enteros tiene una relaciónçon el m.c.d., lo que puede ser útil en muchas aplicaciones, por ejemplo, para encontrar soluciones a ciertas ecuaciones diofánticas.

El *Algoritmo de Euclides* es un método ”rápido´´ de hallar el máximo común divisor de

dos enteros , pero también de encontrar la Identidad de Bézout asociada. Para ello se deben seguir dos pasos:

- Ee divide el número mayor entre el menor.
- Ei la división es exacta, el $m.c.d(a,b)$ es el divisor. Si no lo es, dividimos el divisor entre el resto obtenido y se continúa de esta forma hasta obtener una división exacta, siendo el último divisor el $m.c.d(a,b)$.

Veamos el algoritmo mediante un ejemplo práctico:

Ejemplo 6.

Hallar el $m.c.d(656,848)$:

solución:

$$848 = 1{\cdot}656 + 192$$

$$656 = 3{\cdot}192 + 80$$

$$192 = 2{\cdot}80 + 32$$

$$80 = 2{\cdot}32 + 16$$

$$32 = 2{\cdot}16 + 0$$

El último resto no nulo es $16 = m.c.d(656,848)$. Reutilizando ahora estas ecuaciones (secuencialmente desde la penúltima a la primera) se llega a la Identidad de Bézout.

$$16 = 1{\cdot}80{-}2{\cdot}32$$

$$16 = 1{\cdot}80{-}2{\cdot}(192{-}2{\cdot}80) = 5{\cdot}80{-}2{\cdot}192$$

$$16 = 5{\cdot}(656{-}3{\cdot}192){-}2{\cdot}192 = 5{\cdot}656{-}17{\cdot}192$$

$$16 = 5{\cdot}656{-}17{\cdot}(848{-}1{\cdot}656) = 22{\cdot}656{-}17{\cdot}848$$

La Identidad de Bézout es $16 = 22 \cdot 656 - 17 \cdot 848$, por lo que los coeficientes de Bézout son 22 y -17.

En en el siguiente vídeo se explica cómo se utiliza el algoritmo de Euclides para el cálculo del máximo común divisor y pone un ejemplo:

Accede al vídeo: Algoritmo de Euclides

Ejemplo 7.

a siguiente propiedad se puede probar utilizando el Lema de Bézout:

Si p es un número primo y $p|ab$, entonces o bien $p|a$ o bien $p|b$

Solución:

Supongamos que p no divide a a. Como p es primo, se tiene que $m.c.d.(p, a) = 1$. Por el Lema de Bézout, existen valores enteros s, t tales que $1 = sp + ta$. Multiplicando esta expresión por b se llega a $b = bsp + tba$. Ahora, como por hipótesis se tiene que $p|ab$, sabemos que existe un número entero q tal que $ba = pq$. Volviendo a la igualdad anterior se tiene $b = bsp + tpq = p(bs + tq)$, de donde concluímos que $p|b$.

6.7 Congruencias lineales

Las congruencias lineales son una forma de ecuación modular que se utiliza en la aritmética modular. Una congruencia lineal es una ecuación de la forma:

$$ax \equiv b \, (mod \, m)$$

Donde a, b y m son números enteros y x es la variable desconocida que se quiere encontrar. El símbolo $\equiv$ denota la relación de congruencia, que tal como vimos en el

tema anterior, significa que a, x y b tienen el mismo residuo cuando se dividen por m.

Para resolver una congruencia lineal, se pueden utilizar diferentes métodos, como el algoritmo extendido de Euclides o, tal como veremos a continuación, mediante el teorema chino del resto. La solución de una congruencia lineal es un número entero que satisface la ecuación modular y se encuentra en el rango de 0 a m-1. Dado un número entero a, se llama **inverso modular** de a y lo notamos como a^{-1}, a un valor que satisface

$$aa^{-1} \equiv 1(mod\, m)$$

Se cumple además que $m.c.d.(a, m) = 1$
Por tanto, si conocemos el valor de a^{-1}, podemos resolver la congruencias lineal $ax \equiv b\ (mod\, m)$ multiplicando ambos lados de la ecuación por a^{-1}
Denotamos por $\mathbb{Z}_m^*$ al conjunto de elementos invertibles módulo m. Cabe notar que , si m es primo, $\mathbb{Z}_m^* = \mathbb{Z}_m - [0]$.

En la práctica, si m es un número pequeño, se puede buscar el inverso de un número por tanteo. Por ejemplo, $[2]^{-1} = [3]$ en $\mathbb{Z}_5$ ya que $[2 \cdot 3] = [6] = [1]$. Sin embargo, el método de tanteo puede resultar tedioso si m es un número grande. En esos casos, puede utilizarse el algoritmo de Euclides (visto en el tema anterior) para obtenerlo. Así, como $m.c.d.(a, m) = 1$, sabemos que existen enteros s, t tales que $1 = as´mt$ y ell inverso buscado es $[2]^{-1} = s$.A continuación lo vemos en un ejemplo.

Ejemplo 8.

Obtener el inverso de $[6]$ en $\mathbb{Z}_{17}$ utilizando el algoritmo de Euclides.

Solución: Como 17 es un número primo, sabemos que el inverso modular de $[6]$ existe.

$$17 = 2 \cdot 6 + 5$$

$$6 = 1 \cdot 5 + 1$$

Deshaciendo las igualdades de abajo a arriba se tiene:

$$1 = 6-1 \cdot 5 = 6-1 \cdot (17-2 \cdot 6) = 3 \cdot 6-1 \cdot 17$$

Lo que nos indica que $[6]^{-1} = 3$. En efecto, $[3 \cdot 6] = [18] = 1$.

Ejemplo 9.

¿Cuáles son las soluciones de la congruencia lineal $6x \equiv 7(mod\ 17)$?

Solución: Según el ejemplo anterior, sabemos que $[6]^{-1} = 3$, por tanto, podemos multiplicar ambos lados de la ecuación por3, ya que se cumple que $[6]^{-1} \cdot [6]$ es $1(mod\ 17)$. Por tanto, quedaría:

$$6 \cdot 3x \equiv 7 \cdot 3(mod\ 17)$$

Como $[18 \equiv 1\ (mod\ 17)$ y $[21 \equiv 4\ (mod\ 17)$ entonces $x \equiv 21 \equiv 4\ mod(17)$. Es decir, la solución será todos aquello x tales que x $equiv 4\ mod(17)$, es decir: $4,\ 21,\ 38 \ldots y\ -13, -30,\ \ldots$

6.8 Teorema chino del resto

El teorema chino del resto es un resultado importante de la aritmética modular que establece que, dadas varias congruencias lineales, se puede encontrar una solución única que las satisfaga simultáneamente.

Sean $m_1,\ m_2,\ \ldots,\ m_n$ primos relativos mayores que uno y sean $a_1,\ a_2,\ \ldots,\ a_n$ enteros arbitrarios. El teorema chino del resto afirma que el sistema de ecuaciones lineales congruentes de la forma:

$$\left.\begin{aligned} x &\equiv a_1 (mod\, m_1) \\ x &\equiv a_2 (mod\, m_2) \\ &\dots \\ x &\equiv a_n (mod\, m_n) \end{aligned}\right\}$$

donde $m_1,\ m_2,\ ...,\ m_n$ son enteros positivos que son coprimos dos a dos, es decir, no tienen factores comunes distintos de 1, entonces existe una única solución x, con $0 \leq x < m$, que satisface simultáneamente todas las congruencias.

El teorema chino del resto proporciona un método sistemático para encontrar la solución a este sistema de congruencias lineales utilizando la aritmética modular y el algoritmo extendido de Euclides.

Es decir, dado el número aa $mod\ \ m$, con $0 \leq a < m$, podemos:

- Descomponer m en factores primos relativos $m = m_1 m_2 \cdots m_n$
- Descomponer $a_1 = a\ mod\, m_i$ para $i = 1, 2, ..., n$

Esta descomposición es especialmente interesante cuando el número original a es demasiado grande para ser tratado por un ordenador ya que se cumple que: $a|modn \iff (a_1\ mod\, m_1, a_2\ mod\, m_2, ...a_n\ mod\, m_n)$ El algoritmo de resolución dice que:

$$x = a_1 q_1 r_1 + a_2 q_2 r_2 + \cdots + a_n q_n r_n\ mod(m)$$

Donde $q_i = \frac{m}{m_1}$ y $r_i = [q_i]_{m_i}^{-1}$ para $1 \leq i \leq n$. Este teorema nos permite realizar operaciones de aritmética modular con números más grandes de los que puede representar un ordenador. A continuación, se muestra un ejemplo de aplicación del teorema chino del resto.

Ejemplo 10.

Encontrar ? de modo que:

$$\left.\begin{aligned} x &\equiv 2\ (mod\ 5) \\ 2x &\equiv 1\ mod\ (7) \\ 3x &\equiv 4(mod\ 11) \end{aligned}\right\}$$

Solución:

En primer lugar, simplificamos el sistema de tal forma que los coeficientes que acompañan a x sean 1. Como $[2]_7^{-1} = [4]_7\ y\ [3]_{11}^{-1} = [4]_7$, multiplicando la segunda y tercera ecuación por 4, se llega al sistema equivalente:

$$\left.\begin{aligned} x &\equiv 2\ mod\ (5) \\ x &\equiv 4\ mod\ (7) \\ x \equiv 16\ mod(11) &= 5\ mod\ (11). \end{aligned}\right\}$$

Como $5, 7, 11$ son primos relativos, podemos aplicar el Teorema Chino del Resto para llegar a una solución. Utilizando la notación anterior, $m = 5{\cdot}7{\cdot}11 = 385$,

$$a_1 = 2, q_1 = \frac{385}{5} = 77\ y\ r_1 = [q_1]_5^{-1} = [77]_5^{-1} = [2]_5^{-1} = 3,$$
$$a_2 = 4, q_2 = \frac{385}{7} = 55\ y\ r_2 = [q_2]_7^{-1} = [55]_7^{-1} = [6]_7^{-1} = 6,$$
$$a_3 = 5, q_3 = \frac{385}{11} = 35\ y\ r_3 = [q_3]_{11}^{-1} = [35]_{11}^{-1} = [2]_{11}^{-1} = 6$$

Con todo esto se tiene que:

$$\begin{aligned} x &= a_1q_1r_1 + a_2q_2r_2 + a_3q_3r_3\ mod(m) \\ &= 2 \cdot 77 \cdot 3 + 4 \cdot 55 \cdot 6 + 5 \cdot 55 \cdot 6\ mod(385) = 2832\ mod(385) \\ &= 137\ mod(385) \end{aligned}$$

Y finalmente, son solución del problema los $x = 137 + 385k$ con k cualquier número natural.

6.9 El pequeño teorema de Fermat

Otra de las aplicaciones prácticas de la aritmética modular, viene de la mano del pequeño teorema de Fermat. Este teorema, establece que si p es un número primo y a es un número entero no divisible por p, entonces a elevado a la $(p-1)$ es congruente con 1 módulo p:

Teorema 3

Si p es un número primo y a es un número entero no divisible por p, entonces se cumple que:

$$a^{p-1} \equiv 1 \, mod(p)$$

Y además, se tiene que:

$$a^p \equiv a \, mod(p)$$

Este teorema es extremadamente útil en teoría de números y criptografía, ya que proporciona una forma sencilla de verificar si un número es probablemente primo. También se utiliza para generar claves criptográficas y cifrar mensajes. también resulta especialmente útil para computar el resto en módulo p de potencias con exponentes muy grandes. Veamos un ejemplo:

Ejemplo 11.

Utilizar el Pequeño teorema de Fermat para probar que el número

$$55^{100} + 55^{101} + 55^{102}$$

es múltiplo de 13. **Solución**:

Probar este enunciado es equivalente a demostrar que $55^{100} + 55^{101} + 55^{102} \equiv 0 \, mod(13)$.

Como $[55]_{13} = [3]_{13}$, podemos transformar el enunciado en demostrar $3^{100} + 3^{101} + 3^{102} \equiv 0 \, mod(13)$. Como $m.c.d(13, 3) = 1$ aplicando el Pequeño Teorema de Fermat se tiene que $3^{12} = 1 \, mod(13)$. Ahora, hallamos el cociente y resto de

dividir $100, 101$ y 102 por 12 y procedemos como sigue:

$$3^{100} = 3^{12 \cdot 8+4} = (3^{12})^8 \cdot 3^4 \equiv 1^8 \cdot 3^4 \, mod(13) \equiv 81 \, mod(13) \equiv 3 \, mod(13),$$
$$3^{101} = 3^{12 \cdot 8+5} = (3^{12})^8 \cdot 3^5 \equiv 1^8 \cdot 3^5 \, mod(13) \equiv 243 \, mod(13) \equiv 9 \, mod(13),$$
$$3^{102} = 3^{12 \cdot 8+6} = (3^{12})^8 \cdot 3^6 \equiv 1^8 \cdot 3^6 \, mod(13) \equiv 729 \, mod(13) \equiv 0 \, mod(13),$$

La suma de los tres números es $3 + 9 + 1 \, mod(13) \equiv 13 \, mod(13) \equiv 0 \, mod(13)$.

Definición 8

Sea b un entero positivo. Si n es un entero positivo compuesto y $b^{-1} \equiv 1 \, mod(n)$, entonces n se dice que es un *pseudoprimo* para la base b.

Ejemplo 12.

El entero 341 es un pseudoprimo para la base 2, ya que es compuesto $(341 = 11 \cdot 13)$ y además, se puede comprobar que:

$$2^{240} \equiv 1 \, mod(341)$$

6.10 Raíz primitiva y logaritmo discreto

La raíz primitiva de un número primo p es un número entero r tal que cualquier otro número entero módulo p puede expresarse como una potencia de r:

$$\forall a \in \mathbb{Z}_p - \{0\} \, , \, \exists e \, \in \mathbb{Z}_p - \{0\} \, / r^e = a \, mod(p)$$

Es decir, para cualquier entero a entre 1 y $p - 1$, existe un número entero e tal que $a \equiv r^e mod(p)$. Esto es, todos los elementos de $\mathbb{Z}_p$ excepto el cero se pueden escribir como r^e, lo que quiere decir que existe una relación biyectiva entre a y e.
Un importante hecho de la teoría de números es que si p es primo, entonces existe al menos una raíz primitiva en $\mathbb{Z}_p$.

Ejemplo 13.

Probar que $a = 3$ es una raíz primitiva módulo 5 ¿es la única?

En primer lugar, se tiene que $\mathbb{Z}_5^* = \{[1], [2], [3], [4]\}$ por ser 5 un número primo.

Ahora bien:

$$3^1 = 3\, mod(5), 3^2 = 4\, mod(5), 3^3 = 2\, mod(5), 3^4 = 1\, mod(5)$$

Generando así todo $\mathbb{Z}_5^*$ al multiplicar por si mismo $3\, mod(5)$.

Es fácil ver que $a = 2$, también es una raíz $mod(5)$ mientras que $a = 1$ o $a = 4$ no lo son.

El logaritmo discreto es el problema de encontrar el exponente e en la expresión anterior. Dado un número entero a, una raíz primitiva r y un número primo p, el **logaritmo discreto** es el entero e tal que $a \equiv r^e\ mod(p)$. El *problema del logaritmo discreto* es un problema que dado un primo p, una raíz primitiva r y un entero $a \in \mathbb{Z}_p - \{0\}$, se busca conocer e, es decir, el logaritmo discreto de a en módulo p.

Ejemplo 14.

Hallar una raíz primitiva para el número primo $p = 11$ y calcular el logaritmo discreto de 7 en base 2.

solución: En primer lugar, comprobamos que $r = 2$ es una raíz primitiva para el número primo 11. Para ello buscamos los los elementos generados por $2\, mod(11)$,

elevando 2 a diferentes potencias y reduciendo el resultado a $mod(11)$, es decir:

$$2^1 \equiv 2\ mod(11)$$
$$2^2 \equiv 4\ mod(11)$$
$$2^3 \equiv 8\ mod(11)$$
$$2^4 \equiv 5\ mod(11)$$
$$2^5 \equiv 10\ mod(11)$$
$$2^6 \equiv 9\ mod(11)$$
$$2^7 \equiv 7\ mod(11)$$
$$2^8 \equiv 3\ mod(11)$$
$$2^9 \equiv 6\ mod(11)$$
$$2^{10} \equiv 1\ mod(11)$$

Observamos que los elementos generados por 2 son $\{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}$. Como hay 10 elementos en el grupo, y no hay ningún número menor que 10 que genere todos los elementos del grupo, concluimos que 2 es una raíz primitiva de 11.

Se puede comprobar que el número 3 también podría haber sido una raíz primitiva de 11, siendo los elementos generados por 3 el$\{3, 9, 5, 4, 1\}$. Y nuevamente, como hay 5 elementos en el grupo, y no hay ningún número menor que 5 que genere todos los elementos del grupo, concluimos que 3 también es una raíz primitiva de 11.

Ahora, para calcular el logaritmo discreto de $a = 7$ en base $r = 2\ mod(11)$, debemos encontrar el entero e tal que $2^e \equiv 7\ mod(11)$. Usando la definición de

logaritmo discreto, podemos escribir:

$$2^e \equiv 7\ mod(11)$$
$$2^2 \equiv 4\ mod(11)$$
$$2^3 \equiv 8\ mod(11)$$
$$2^4 \equiv 5\ mod(11)$$
$$2^5 \equiv 10\ mod(11)$$
$$2^6 \equiv 9\ mod(11)$$
$$2^7 \equiv 7\ mod(11)$$

Por lo tanto, el logaritmo discreto de $a = 7$ en base $r = 2\ mod(11)$ es $r = 7$. Es decir, $2^7 \equiv 7\ mod(11)$.

En el anterior ejemplo, hemos encontrado el logaritmo discreto de un número mediante el método de tanteo. No existe ningún algoritmo conocido con coste computacional polinómico para resolver el problema en general. El hecho de que $a^k\ mod(m)$ pueda ser calculado fácilmente pero no así el valor de k para el que $a^k = b\ mod(m)$ ha sido explotado y utilizado en la construcción de multitud de sistemas criptográficos para cifrar mensajes de manera segura.

6.11 Criptografía. Algoritmo Diffie-Hellman y RSA

Para terminar el tema de aplicaciones de la aritmética modular, se presentan dos ejemplos de aplicación de esta en el campo de la criptografía.

La criptografía es el estudio de los principios y técnicas utilizados para proteger la información. Uno de los principales objetivos de la criptografía es garantizar la confidencialidad de los datos, es decir, impedir que terceros no autorizados puedan acceder y

comprender la información transmitida.

El algoritmo de Diffie-Hellman es un protocolo criptográfico conocido como de *clave pública*, utilizado para establecer una clave secreta compartida entre dos usuarios a través de un canal inseguro. Fue desarrollado por Whitfield Diffie y Martin Hellman en 1976 y se considera uno de los primeros algoritmos de clave pública. Es un algoritmo de intercambio de claves cuya seguridad se basa en la dificultad de calcular el logaritmo discreto de un número grande, en comparación con calcular su exponenciación.

El protocolo de intercambio entre A y B es el siguiente:

- A elige un número entero grande x aleatoriamente (que no debe mostrar), calcula $(X = r^x)\ mod\ (p)$ y envía X a B.
- B elige un número entero grande y aleatoriamente (que no debe mostrar), calcula $(Y = ry)\ mod(p)$ y envía Y a A.
- A calcula $(K = Y^x)\ mod(p)$.
- B calcula $(K' = X^y)\ mod(p)$

Y ahora resulta que se cumple que:

$$(r^{xy} \equiv X^y \equiv Y^x \equiv K \equiv K')\ mod(p)$$

Con lo que $(K \equiv K')\ mod(p)$ es la clave de sesión que pueden usar A y B para comunicarse.

En en el siguiente vídeo se explica cómo se utiliza el algoritmo algoritmo criptográfico de Diffie-Hellman y pone un ejemplo.:

Accede al vídeo: Algoritmo de Diffie-Hellman

RSA es otro algoritmo criptográfico que también se basa en la criptografía de clave pública. Fue inventado por Ron Rivest, Adi Shamir y Leonard Adleman en 1977. RSA se basa en el problema de la factorización de números enteros grandes, que es considerado un problema difícil de resolver. RSA utiliza dos claves: una pública, que puede ser compartida con cualquier persona, y una privada, que solo el propietario de la clave puede usar para descifrar los datos cifrados. RSA se utiliza ampliamente para la seguridad en línea, como la protección de contraseñas, la autenticación de identidad y la protección de datos en tránsito. A continuación se explica como funciona el cifrado RSA mediante un ejemplo sencillo:

- Generación de claves:

  En primer lugar, se generan dos números primos grandes diferentes; en este caso, por sencillez, elegimos $p = 7$ y $q = 11$. Luego, se calcula su producto, $n = p \times q$, que en este caso es $n = 77$. Este número n se utiliza como el módulo para el cifrado y el descifrado.

  A continuación, se calcula la función de Euler $\varphi(n) = (p-1)(q-1)$, que en este caso es $\varphi(77) = 6 \times 10 = 60$. La función de Euler es importante en la elección de la clave pública.

  Luego, se elige un número entero e que sea menor que $\varphi(n)$ y que no tenga factores comunes con $\varphi(n)$. Digamos que elegimos $e = 13$.

  Finalmente, se calcula un número $d = e^{-1}$ que es el inverso modular de $e\, mod(\varphi(n))$. En otras palabras, d es un número tal que $e \times d1\ mod(\varphi(n))$. En este caso, podemos calcular $d = 37$.

  Así, la clave pública es el par $(n, e) = (77, 13)$ y la clave privada es el número $d = 37$.

- Cifrado:

  Supongamos que queremos cifrar el mensaje $M = 42$. Primero, convertimos el mensaje a un número entero m que sea menor que n. En este caso, $m = 42$.

  Luego, ciframos el mensaje usando la clave pública (n, e) de la siguiente manera:

$$c \equiv m^e\ mod(n)$$

En este caso, $c \equiv 42^{1}3\ (mod 77) \equiv 19\ mod(77)$. Por lo tanto, el mensaje cifrado es $c = 19$.

- Descifrado:

  Para descifrar el mensaje cifrado c, usamos la clave privada d de la siguiente manera:

  $$m \equiv c^{b}\ mod(n)$$

  En este caso, $m = 19^{37}\ mod(77) \equiv 42\ mod(77)$. Por lo tanto, el mensaje original M era 42.

En en el siguiente vídeo se explica cómo se utiliza el algoritmo criptográfico RSA y pone un ejemplo.

Accede al vídeo: Algoritmo RSA

6.12 Referencias bibliográficas

Rosen, K. H., & Morales, J. M. P. (2004). Matemática discreta y sus aplicaciones.

Koshy, T. (2004). Discrete mathematics with applications. Elsevier.

Grimaldi, R. P. (2006). Discrete and Combinatorial Mathematics, 5/e. Pearson Education India.

Grimaldi, R.P., (2004). Discrete and combinatorial mathematics (5th ed). Pearson.

Hunter, D.J., (2017). Essentials of discrete mathematics (3rd edition). Jones & Bartlett and Hall Learning.

6.13 Cuaderno de ejercicios

Ejercicio 1.

Encuentra el mínimo común múltiplo y máximo común divisor de:

- (30,18).
- (−27,93).
- (0,32).

Ejercicio 2.

Utilizando el algoritmo de Euclides, calcula el m.c.d (210,45).

Ejercicio 3. Razonar si 17 divide a los siguientes enteros: $68, 84, 357, 1001$.

Ejercicio 4.

Obtener el cociente y el resto de dividir -11 entre 3.

Ejercicio 5.

Encuentra todos los valores enteros x que cumplen la congruencia $4x^2 + 19 \equiv mod(5)$.

Ejercicio 6.

Probar mediante congruencias que $3^{2n+5} + 2^{4n+1}$ es divisible por 7 para cualquier entero $n > 0$.

Ejercicio 7.

¿Se puede encontrar un número entero positivo menor que 105 si conoces los residuos respecto a $3, 5\ y\ 7$? Si es así, encuentra los posibles resultados con restos $2,\ 1,\ y\ 4$, respectivamente.

Ejercicio 8.

Resuelve el siguiente acertijo propuesto por el matemático chino Sun-Tsu (Siglo IV a.C.):

«Hay una cierta cantidad de cosas cuyo número es desconocido. Si contamos en ternas, no sobran dos; si contamos de cinco en cinco, nos sobran tres; y si contamos de siete en siete, nos sobran dos. ¿Cuál es la cantidad?».

Ejercicio 9. Utilizando el pequeño teorema de Fermat, resuelve la congruencia $x^{39} \equiv 3\, mod(13)$.

Ejercicio 10.

Obtener el inverso modular de $3\, mod(7)$.

Solución:

Como $m.c.d(3,7) = 1$, se sabe que existe un inverso de 3 módulo 7. Median1e el algoritmo ele Euclides podemos calcular rápidamente el máximo común divisor de 1 y 7:

$$7 = 2{\cdot}3 + 1.$$

De esta igualdad se tiene que

$$-2{\cdot}3 + 1{\cdot}7 = l$$

Esto muestra que -2 es un inverso de 3 módulo 7. (Observe que todo entero congruente con -2 módulo 7 es también un inverso de 3, como pueden ser $5,\ -9,\ 12,\ etc$).

6.14 Soluciones cuaderno de ejercicios

Solución 1.

- m.c.d (30,18)= 6; m.c.m (30,18)= 90
- m.c.d −27,93)=3; m.c.m −27,93)=837
- m.c.d (0,32)=0; m.c.m (0,32)=0

Solución 2.

Tenemos que realizar la división entera:

$$210 = 4{\cdot}45 + 30$$

Si el residuo es 0, hemos terminado. Si no, hay que repetir el proceso con 45 y 30, ya que $m.c.d.(210, 45) = m.c.d.(45, 30)$

$$45 = 1{\cdot}30 + 15.$$

$$30 = 2{\cdot}15 + 0.$$

El resultado final es:

$m.c.d.(210, 45) = m.c.d.(45, 30) = m.c.d.(30, 15) = m.c.d.(15, 0) = 15.$

Solución 3.

Únicamente divide a 68 y 357.

Solución 4.

Se tiene que:

$$-11 = 3 \cdot (-4) + 1$$

Por tanto, el cociente de (-11) entre 3 es $(-4 = -11\ div\ 3)$ y el resto es $1 =$

$-11 mod\ 3$. Téngase en cuenta que el resto no puede ser negativo. Por tanto, el resto no es -2, a pesar de que $-11 = 3\cdot(-3)-2$ puesto que $r = -2$ no satisface la desigualdad $0 \leq r \leq 3$.

Solución 5.

Primero buscamos una solución $0 \leq \ < 5$. Al operar en congruencias, las sumas y productos se comportan de forma usual. Además, podemos sumar o restar 5 a cualquier número y el resultado será el mismo. Así pues: $19 \equiv -1\ mod(5)$, por lo que nos queda la congruencia $x^2 \equiv -1\ mod(5)$.
Las potencias se comportan de forma distinta, pero como x solo puede tomar 5 valores distintos, podemos comprobarlos todos. Obtenemos que $2^2 \equiv -1\ mod(5)$ y $3^2 \equiv -1\ mod(5)$.
Por lo tanto, las soluciones son $\ = 2 + 5n$ y $\ = 3 + 5n$, con n entero.

Solución 6.

Tenemos que ver que $3^{2n+5} + 2^{4n+1} \ = 0\ mod(7)$. Podemos hacer las siguientes simplificaciones:

$$3^{2n+5}+2^{4n+1} = 3^5\cdot 3^{2n}+2\cdot 2^{4n} \equiv 243\cdot 9^n+2\cdot 16^n \equiv 5\cdot 2^n+2\cdot 2^n \equiv 7\cdot 2^n \equiv 0\, mod(7)$$

Solución 7.

Por el teorema chino del resto, existe una única solución entre $0 \leq x < 3 \cdot \cdot 5\cdot 7 = 105$. Por lo tanto, sí que existe este número y es único. Para el caso concreto tenemos que resolver:

$$\begin{cases} X \equiv 2\ mod(3) \\ X \equiv 1\ mod(5) \\ X \equiv 4\ mod(7) \end{cases}$$

De la primera congruencia deducimos que $\ = 2 + 3\cdot n$. Poniendo esta condición en la segunda, deducimos que $n \equiv 3\ mod(5)$, es decir, $\ = 2 + 3\cdot(3 + 5\cdot m)$.

Poniendo esta condición en la última ecuación deducimos que $m = 0\, mod(7)$, es decir, $= 2 + 3{\cdot}(3 + 5{\cdot}7{\cdot}k)$. Para obtener un valor entre 0 y 105 hay que escoger la solución con $k = 0$, de donde se obtiene $x = 11$.

Solución 8.

Este problema se puede resumir en el siguiente sistema de congruencias:

$$\begin{cases} X \equiv 2\, mod(3) \\ X \equiv 1\, mod(5) \\ X \equiv 2\, mod(7) \end{cases}$$

De la primera congruencia deducimos que $x \equiv 2 + 3{\cdot}n$. Poniendo esta condición en la segunda, deducimos que $n \equiv 2\, mod(5)$, es decir,$x \equiv 2 + 3{\cdot}(2 + 5{\cdot}m)$. Poniendo esta condición en la última ecuación deducimos que $m \equiv 0\, mod(7)$, es decir$x \equiv 2 + 3{\cdot}(2 + 5{\cdot}7{\cdot}k) = 8 + 105k$.

Como no nos dan más información, por cada k entero positivo tenemos una solución válida. Las soluciones negativas no son apropiadas, ya que se refiere a cantidad de algo.

Solución 9.

Para usar el pequeño teorema de Fermat, necesitamos que el exponente sea 12.

$$x^{39} \equiv x^{3{\cdot}12+3} \equiv (x^{12})^3 \cdot x^3 \equiv 1^3 \cdot x^3 \equiv 1\, mod(13)$$

Comprobando los posibles valores entre 0 y 12, vemos que las tres familias de soluciones son: $x = 1 + 13n;\ x = 3 + 13n;\ x = 9 + 13n$, con n entero.

Solución 10.

Como $m.c.d(3, 7) = 1$, se sabe que existe un inverso de 3 módulo 7. Median1e el algoritmo de Euclides podemos calcular rápidamente el máximo común divisor de 1 y 7:

$$7 = 2{\cdot}3 + 1.$$

De esta igualdad se tiene que

$$-2{\cdot}3 + 1{\cdot}7 = l$$

Esto muestra que -2 es un inverso de 3 módulo 7. (Observe que todo entero congruente con -2 módulo 7 es también un inverso de 3, como pueden ser $5,\ -9,\ 12,\ etc$).

6.15 A fondo

A fondo

Seguridad, criptografía y comercio electrónico con Java.

Este tutorial lleva a cabo un estudio de las herramientas de programación para la criptografía. Son especialmente interesantes los temas del 3 al 5, donde se trata la teoría de números y las herramientas criptográficas de clave pública.

Accede al tutorial desde el aula virtual o a través de la siguiente dirección web:

http://190.90.112.209/criptografia/Seguridad_criptografia_y_comercio_electronico_con_java.pdf

Máximo común divisor y mínimo común múltiplo

Este vídeo da una visión sencilla y de divulgación de la aritmética modular y la forma en que se calcula el máximo común divisor y el mínimo común múltiplo.

Accede al vídeo desde el aula virtual o a través de la siguiente dirección web:

http://www.youtube.com/watch?v=Evea_X_dSVo

Elementary Number Theory: Primes, congruences and Secrets

Se trata de un documento acerca de los números primos, congruencias, mensajes, secretos y curvas elípticas que se pueden leer de principio a fin. Surgió de los cursos que el autor imparte en Harvard, UC San Diego, y la Universidad de Washington.

Accede al artículo desde el aula virtual o a través de la siguiente dirección web:

http://wstein.org/ent/ent.pdf

6.16 Test

Test

1. Dados los números 0 y 1:

A. Todo entero divide a 0 y a 1.

B. Ningún entero divide a 0 ni a 1.

C. Ningún entero divide a 0 y 1 divide a todos los números.

D. Todo entero divide a 0 y 1 divide a todos los números.

2. Cuál es el m.c.d. (2,-1), y el m.c.d.(0,9):

A. No está definido y 0, respectivamente.

B. 1 y 9, respectivamente.

C. -1 y 9, respectivamente.

D. 1 y no está definido, respectivamente.

3. El teorema fundamental de la aritmética afirma que:

A. La probabilidad de que un número n elegido al azar sea primo no es mayor a $1/ln(n)$.

B. Todo entero mayor que 1 se puede representar de forma única como el producto de números primos.

C. Dado un entero a y un entero positivo d existen enteros únicos q y r tales que $0 \leq r$ y $a = dq + r$.

D. Todo número impar $n > 5$ es la suma de tres primos.

4. El teorema de los números primos, afirma que:

A. La probabilidad de que un número n elegido al azar sea primo no es mayor a 1 / $ln(n)$.

B. Todo entero mayor que 1 se puede representar de forma única como el producto de números primos.

C. Dado un entero a y un entero positivo d existen enteros únicos q y r tales que 0 $\leq r$ y $a = dq + r$.

D. Todo número impar $n > 5$ es la suma de tres primos.

5. El teorema de la división, afirma que:

A. La probabilidad de que un número n elegido al azar sea primo no es mayor a 1 / $ln(n)$.

B. Todo entero mayor que 1 se puede representar de forma única como el producto de números primos.

C. Dado un entero a y un entero positivo d existen enteros únicos q y r tales que 0 $\leq r$ y $a = dq + r$.

D. Todo número impar $n > 5$ es la suma de tres primos.

6. El máximo común divisor y mínimo común múltiplo se relacionan como:

A. {m.c.d(a,b)x+m.c.m(a,b)y: x,y ∈ Z}.

B. {m.c.d(a,b)x · m.c.m(a,b)y: x,y ∈ Z}.

C. ab=m.c.d.(a,b) · m.c.m(a,b).

D. ab=m.c.d.(a,b) + m.c.m.(a,b).

7. El algoritmo de Euclides permite:

A. Obtener los factores de un número eficientemente.

B. Determinar si un número es primo.

C. Calcular el $\mathrm{mcd}(a,b)$ eficientemente.

D. Calcular q y r eficientemente para $a = dq + r$.

8. La identidad de Bézout obtenida para los valores a=30 y b=13 es

A. $1=-3\cdot 30+7\cdot 13$.

B. $3=-3\cdot 30+7\cdot 13$.

C. $1=3\cdot 30-7\cdot 13$.

D. $3=3\cdot 30-7\cdot 13$.

9. ¿Cuál es el propósito del algoritmo de Eratóstenes?

A. Encontrar el mínimo común múltiplo de dos números enteros.

B. Encontrar el máximo común divisor de dos números enteros.

C. Encontrar todos los números primos menores o iguales a un número entero dado.

D Encontrar la raíz cuadrada de un número entero.

10. ¿Cuál de las siguientes afirmaciones es cierta sobre la división por tentativa?

A. Es un método para encontrar todos los divisores de un número entero dado.

B. B Es un método para encontrar el cociente y el residuo de la división entre dos números enteros.

C. Es un método para determinar si un número entero dado es primo o compuesto.

D. Es un método para encontrar el máximo común divisor de dos números enteros.