Estructuras Algebraicas

- Sea A un conjunto no vacío, una función f

$$f: A \times A \mapsto A$$

se llama **ley de composición interna** (operación) sobre A. Además, la imagen $f(a,b)$ se llama el operado de a y b.

- Es usual representar las operaciones internas con algunos símbolos especiales, en vez de letras, como *, Δ, ⊥, entre otros.
- Por definición, si * es una ley de composición interna sobre A, entonces es **cerrada** sobre A, es decir, se cumple que

$$\forall a, b \in A[a * b \in A]$$

1

Estructuras Algebraicas (cont.)

- Si * es una ley de composición interna sobre E, se dice que $(E,*)$ posee una **estructura algebraica**.
- Una **estructura algebraica** es una n-tupla $(a_1,a_2,...,a_n)$, donde a_1 es un conjunto dado no vacío, y $\{a_2,...,a_n\}$ un conjunto de operaciones aplicables a los elementos de dicho conjunto.
- Si * es una ley de composición interna sobre E, se dice que *:
  - Es **asociativa:** para cualesquiera elementos del grupo no importa el orden en que se operen las parejas de elementos, mientras no se cambie el orden de los elementos, siempre dará el mismo resultado.

Si $\forall a, b \in E$ se cumple $(a * b) * c = a * (b * c)$

2

Estructuras Algebraicas (cont.)

- Si * es una ley de composición interna sobre E, se dice que *:
  - Posee **elemento neutro o elemento identidad** (comúnmente denotado como e, letra inicial de la palabra alemana ***einheit***, que significa "unidad"): existe un elemento que al ser operado con cualquier otro, no lo modifica (como el cero en la suma o el 1 en la multiplicación). La unicidad del elemento neutro es fácilmente demostrable.

    Si $\exists e \in \forall a \in A$ tal que $a * e = e * a = a$

  - Tiene **elemento inverso**: todos los elementos del grupo tienen un elemento inverso, con el que al operarse dan por resultado el elemento neutro e. El elemento inverso de uno dado es único.

    Si $\forall a \in A \wedge \exists b \in A$ tal que $a * b = b * a = e$
    en cuyo caso se escribe $a^{-1} = b$

3

Estructuras Algebraicas (cont.)

- Si * es una ley de composición interna sobre A, se dice que *:
  - Es **conmutativa**: para cualesquiera elementos del grupo no importa el orden de los elementos siempre dará el mismo resultado.

    Si $\forall a, b \in A$ se cumple $a * b = b * a$

4

Grupos

- Si G es un conjunto no vacío y * es una operación interna definida sobre G. Se dice que $(G,*)$ es:
  - Un **semigrupo** si * es asociativa.
  - Un **monoide** si es un semigrupo con elemento neutro.
  - Un **grupo** si es un monoide que cumple la propiedad de los inversos, es decir, $(G,*)$ es un grupo si * es cerrada, asociativa, posee elemento neutro y cada elemento tiene inverso.
  - Un **grupo abeliano** o **grupo conmutativo** si es un grupo y se cumple la conmutatividad. En el caso de que no sea un grupo, se dice que la estructura algebraica es conmutativa.

5

Grupos (cont.)

- Notaciones:
  - La notación multiplicativa $\otimes$.
    - Operación: $*$, $\times$, $\bullet$, llamada producto.
    - Elemento neutro: 1.
    - Elemento inverso: x^{-1}.
  - La notación aditiva $\oplus$.
    - Operación: +, llamada suma.
    - Elemento neutro: 0.
    - Elemento opuesto de un elemento x del grupo: $-x$.

6

Grupos (cont.)

- Si $(G,*)$ es un monoide, se tiene que $a^0 = e$, y para n natural, con $n \geq 1$:

$$a^n = a * a^{n-1}$$
$$a^n = a * a * a * \ldots * a$$

• n veces a

- Si además cumple con la propiedad de los inversos, los exponentes negativos se definen como:

$$a^{-n} = (a^{-1})^n$$

7

Grupos (cont.)

- Notar que si el grupo es abeliano se puede escribir

$$(a * b)^{-1} = a^{-1} * b^{-1}$$

- Si el grupo es finito, su **orden** se denota por $o(G)$ y corresponde a la cardinalidad como conjunto.
- Para $n \in N$ con $n \geq 2$, y la relación $\Re$ definida sobre Z por

$a \Re b \Leftrightarrow [\exists k \in Z$ tal que $a - b = nk]$ se define al conjunto $Z_n = Z/\Re$, es decir, Z_n es el conjunto de clases residuales módulo n.

- Sobre estos conjuntos Z_n, se definen las operaciones usuales de suma $\oplus$ y multiplicación $\otimes$ de clases.

8

Grupos (cont.)

- Para todo $n \geq 2$, $(Z_n, \oplus)$ es grupo abeliano y $o(Z_n) = n$.
- $(Z_n^*, \otimes)$ es grupo abeliano si y sólo si n es un número primo. Además, $o(Z_n^*) = n - 1$.
- Sea G un grupo, y un elemento $x \in G$. se dice que G es un **grupo cíclico** generado por x si para cada elemento $y \in G$ existe un $n \in Z$ tal que $y = x^n$.

9

Grupos (cont.)

- **Teorema.** Si G es cíclico entonces es grupo abeliano, y si G es generado por x entonces también es generado por su inverso x^{-1}.
- **Demostración.**

(1)
$y, z \in G \Rightarrow \exists n, m \in Z$ tal que $y = x^n \wedge z = x^m$
$yz = x^n x^m = x^{n+m} = x^{m+n} = x^m x^n = zy$
Es grupo abeliano

(2)
$y \in G \Rightarrow \exists n \in Z$ tal que $y = x^n$
Es decir, $y = (x^{-1})^{-n} \wedge -n \in Z$
G es generado por x^{-1}

10

Grupos (cont.)

- Para el conjunto $X = \{1, \ldots, n\}$, se define el **grupo simétrico S_n** como el conjunto de todas las funciones biyectivas de X en X, dotado con la composición de funciones como operación interna.
- El orden de S_n es $n!$, $o(S_n) = n!$.
  - Al asignar la imagen al primer elemento se tienen n posibilidades al fijar una de éstas, para asignar la imagen del segundo elemento se tienen $n - 1$ posibilidades; así, al fijar las imágenes para hacer la función biyectiva, el número de funciones que se obtiene es $n!$.
- Si p es un número primo y G un grupo, se dice que G es un ***p*-grupo** si su orden es una potencia de p.

11

Subgrupos

- Algunos conjuntos que poseen estructura de grupo, poseen subconjuntos que también tienen esta misma estructura de grupo.
- Si $(G,*)$ es un grupo, $H \subseteq G$ con $H \neq \varnothing$, H se llamará **subgrupo** de G, y se denota por $H < G$, si y sólo si $(H,*)$ es un grupo.
  - Un subgrupo es un subconjunto no vacío del grupo que sea grupo con la operación restringida a sus elementos.
- **Teorema De Lagrange.** El orden del subgrupo es un divisor del orden del grupo.

12

Subgrupos (cont.)

- Una condición necesaria para que $(Z_n^*, \otimes)$ sea grupo es que p sea primo. Así, en el caso que p no es primo no se obtiene la deseada estructura de grupo.
  - Al considerar el subconjunto de Z_n^* formado por las clases residuales que son relativamente primos con n, se obtiene un grupo abeliano.
- El conjunto U_n, definido por $U_n = \{\dot{a} \in Z_n \ / m.c.d.(a,n) = 1\}$ es un grupo abeliano.

13

Anillos

- Un **anillo** es una estructura algebraica formada por un conjunto y dos operaciones que están relacionadas entre sí, mediante la propiedad distributiva, de manera que generalizan las nociones de número, especialmente en el sentido de su "operabilidad".
  - En un anillo se tienen un conjunto no vacío A, y dos operaciones binarias + y •.

14

Anillos (cont.)

- Un anillo es un triple $(A,*,\circ)$, lo cual es una estructura algebraica en la cual A es un conjunto no vacío y $*,\circ: A \times A \to A$ son dos operaciones binarias definidas sobre A que satisfacen las condiciones siguientes:
  - $(A,*)$ es un grupo abeliano.
  - $(A,\circ)$ es un semigrupo.
  - La operación $\circ$ es distributiva respecto a la operación $*$. Esto es, para todo $a,b \in A$

$$\begin{cases} a \circ (b * c) = (a \circ b) * (a \circ c) \\ (a * b) \circ c = (a \circ c) * (b \circ c) \end{cases}$$

15

Anillos (cont.)

- Cuando $(A,\circ)$ es un monoide se dice que A es un **anillo unitario** o **anillo con unidad** que representaremos por 1 (elemento neutro del producto).
- Cuando $(A,\circ)$ es un semigrupo conmutativo, se dice que A es **anillo conmutativo** o **anillo abeliano**.

16

Anillos (cont.)

- Para trabajar con una notación más familiar, el anillo $(A,+,\bullet)$, en el cual:
  - El neutro de $(A,+)$ se denota 0, y para todo $x \in A$, a su inverso (para la operación +) se denotará $-x$.
  - Si la operación $\bullet$ posee neutro en A, éste se denotará por 1 y se dice que $(A,+,\bullet)$ es un **anillo con unidad**.
  - Si $x \in A$ posee inverso para la operación $\bullet$, éste se denotará por x^{-1}. Si $\bullet$ es conmutativa, $(A,+,\bullet)$ se llamará **anillo conmutativo**.

17

Anillos (cont.)

- El ejemplo más sencillo y representativo de estructura de anillo se encuentra en $(Z,+,\bullet)$, el anillo de los enteros. Este anillo tiene unidad y es conmutativo.
- Por similitud con $(Z,+,\bullet)$, cuando tratemos con un anillo unitario cualquiera, en general se refiere a la suma y al producto como primera y segunda operación, respectivamente, y se utiliza el 0 y el 1 como neutros respectivos.
  - Para abreviar la notación, se escribe ab en lugar de $a \bullet b$.

18

Anillos (cont.)

- Los axiomas de anillo son una abstracción del comportamiento de los números enteros respecto de las operaciones aritméticas elementales: la suma y el producto.
- Otra clase importante de anillos abelianos unitarios finitos es $(Z_n,+,\bullet)$ el anillo de los enteros módulo n.

19

Anillos (cont.)

- Sea $(A,+,\bullet)$ un anillo, entonces:
  - $(\forall x \in A)\ 0 \bullet x = x \bullet 0 = 0$.
  - $(\forall x,y \in A)\ -(x \bullet y) = (-x) \bullet y = x \bullet (-y)$.
  - $(\forall x,y \in A)\ (-x) \bullet (-y) = x \bullet y$.
  - Si el anillo posee unidad, entonces $(\forall x \in A)\ -x = (-1) \bullet x = x \bullet (-1)$.
- La **ley de simplificación** es otra propiedad importante que cumplen los números enteros, es decir, para todo $a,b,c \in Z^* = Z - \{0\}$ se verifica $ab = ac \Rightarrow b = c$.

20

Anillos (cont.)

- La propiedad de ley de cancelación está relacionada con la definición:
  - El anillo $(A,+,\bullet)$ admite divisores de cero si existen $a,b \in A^* = A - \{0\}$ tales que $ab = 0$.
    - Los elementos [2] y [3] de Z_6 son dos divisores de cero.
    - Los divisores de cero de un anillo Z_n son aquellas clases cuyos elementos no son primos relativos de n ($mcd(n,a) \neq 1$).
- **Teorema.** Sea el anillo $(A,+,\bullet)$, entonces es válida la ley de cancelación si y sólo si no tiene divisores de cero.
  - Se llama **dominio de integridad**, a un anillo conmutativo unitario que no contiene divisores de cero.

21

Si una operación * respecto de los elementos de un conjunto G que se escribe: (G, *), verifica que:

1) $G^2 \rightarrow G$ * es una Ley de composición interna en G

Definida una operación * si el resultado de operar dos elementos cualesquiera de G con * es otro elemento de G, hay L.C.I.

2) $\forall a, \forall b, \forall c : a, b, c \in G \Rightarrow (a * b) * c = a * (b * c)$ Asociativa

Definida una operación * si con tres elementos cualesquiera de G la operación * responde a la propiedad asociativa (G, *) tiene estructura de semi-grupo si además

3) $\exists e \in G / \forall a : a \in G \Rightarrow a * e = e * a = a$ Existe Elemento Neutro

Definida una operación * si en el conjunto G existe al menos un elemento "e", que al operarlo con cualquier otro elemento "a" de G, resulta el mismo elemento "a"

4) $\forall a : a \in G, \exists a' \in G / a * a' = a' * a = e$ Existe Elemento Inverso

Definida una operación * si para cada elemento de G existe al menos un elemento a´que al operar con a dá como resultado el neutro e (G, *) tiene estructura de grupo

Si además de cumplirse las cuatro condiciones anteriores - lo que hace a (G,*) Grupo -

5) $\forall a, \forall b : a, b \in G \Rightarrow a * b = b * a$ Conmutativa $(G, *)$ tiene estructura de grupo abeliano o grupo conmutativo

Sea una estructura algebraica definida en un conjunto G con dos leyes de composición * y •
$(G, * \bullet)$ es Anillo si . . .

1) $(G, *)$ es Grupo abeliano
2) $(G, \bullet)$ es semi Grupo
3) • es distributivo a izquierda y derecha respecto de *
$\forall a, \forall b, \forall c \in G$: $a \bullet (b * c) = (a \bullet b) * (a \bullet c)$
$(b * c) \bullet a = (b \bullet a) * (c \bullet a)$

Si la segunda ley de composición es conmutativa, $(G, * \bullet)$ es Anillo Conmutativo

Si $(G * \bullet)$ es Anillo,y además posee elemento neutro respecto de • $(G * \bullet)$ es Anillo con Unidad

Un Anillo con unidad cuyos elementos no nulos son inversibles se llama **Anillo con división**

Si un Anillo con división es conmutativo, se llama **Cuerpo**

1) $(G, *)$ es Grupo abeliano
2) $(G, \bullet)$ es Grupo abeliano, salvo que el 0 no es inversible
3) • es distributivo respecto de *

Ejemplo:
$(Z, * \bullet)$ donde * es la adición (suma) y • es el producto ordinario **No es cuerpo**, pues los únicos elementos no nulos que admiten inverso multiplicativo son 1 y – 1

$(R, * \bullet)$ donde * es la adición (suma) y • es el producto ordinario **Es Cuerpo**

Inversos en Z_n

- Si $a * x \equiv 1 \bmod n$
  - se dice que x es el inverso multiplicativo de a en Z_n y se denotará por a^{-1}.
- No siempre existen el inverso de un elemento en Z_n. Por ejemplo, si n = 6, en Z_6 no existe el inverso del 2, pues la ecuación $2*x \equiv 1 \bmod 6$ no tiene solución.
- Si n es un número primo p, entonces todos los elementos de Z_p salvo el cero tienen inverso. Por ejemplo, en Z_5 se tiene que:

  $1^{-1} \bmod 5 = 1$; $2^{-1} \bmod 5 = 3$, $3^{-1} \bmod 5 = 2$; $4^{-1} \bmod 5 = 4$.

Existencia del inverso por primalidad

$\exists$ inverso a^{-1} en mod n *si y sólo si* mcd (a, n) = 1

Si mcd (a,n) = 1, el resultado de a∗i mod n (para i todos los restos de n) serán valores distintos dentro del cuerpo n.

$$\text{mcd}(a, n) = 1 \quad \Rightarrow \quad \exists\, x \,!\ \ 0 < x < n \ \ / \ a * x \bmod n = 1$$

Sea: a = 4 y n = 9. Valores de i = {1, 2, 3, 4, 5, 6, 7, 8}

4∗1 mod 9 = 4	4∗2 mod 9 = 8	4∗3 mod 9 = 3
4∗4 mod 9 = 7	4∗5 mod 9 = 2	4∗6 mod 9 = 6
4∗7 mod 9 = 1	4∗8 mod 9 = 5	

Inexistencia de inverso (no primalidad)

- Si mcd (a, n) $\neq$ 1
- No existe ningún x que $0 < x < n$ / $a * x \bmod n = 1$
- Sea: a = 3 y n = 6 Valores de i = {1, 2, 3, 4, 5}
- $3*1 \bmod 6 = 3$ $3*2 \bmod 6 = 0$ $3*3 \bmod 6 = 3$
- $3*4 \bmod 6 = 0$ $3*5 \bmod 6 = 3$
- No existe el inverso para ningún resto del cuerpo.

Conjunto reducido de restos CRR

El conjunto reducido de restos, conocido como CRR de n, es el subconjunto {0, 1, ... n_i, ... n-1} de restos, primos con el grupo n.

Si n es primo, todos los restos serán primos con él.

Como el cero no es una solución, entonces:

CRR = {1, ..., n_i, ... n-1} / mcd (n_i, n) = 1

Ejemplo: CRR mod 8 = {1, 3, 5, 7}

CRR mod 5 = {1, 2, 3, 4}

Utilidad del CRR

- El conocimiento del CRR permite aplicar un algoritmo para el cálculo del inverso multiplicativo de un número x dentro de un cuerpo n a través de la función $\phi(n)$, denominada Función de Euler o Indicador de Euler.

Función de Euler $\phi(n)$

El Indicador o Función de Euler $\phi(n)$ nos indica el número de elementos del CRR.
Podremos representar cualquier número n de estas cuatro formas:

a) n es un número primo.
b) n se representa como $n = p^k$ con p primo y k entero.
c) n es el producto $n = p*q$ con p y q primos.
d) n es un número cualquiera, forma genérica:

$$n = p_1^{e1} * p_2^{e2} * ... * p_t^{et} = \prod_{i=1}^{t} p_i^{ei}$$

Función $\phi(n)$ de Euler cuando n = p

Si n es primo, $\phi(n)$ será igual a CCR menos el 0.

$$\phi(n) = n - 1$$

Si n es primo, entonces $\phi(n)$ = CCR - 1 ya que todos los restos de n, excepto el cero, serán primos entre sí.

- Ejemplos

(7) = {1,2,3,4,5,6} seis elementos
∴ $\phi(7) = n - 1 = 7-1 = 6$
$\phi(11) = 11-1 = 10$; $\phi(23) = 23-1 = 22$

Función $\phi(n)$ de Euler cuando $n = p^k$

$n = p^k$ (con p primo y k un entero)

$$\phi(n) = \phi(p^k) = p^k - p^{k-1} \qquad \phi(p^k) = p^{k-1}(p-1)$$

De los p^k elementos del CCR, restaremos todos los múltiplos $1*p$, $2*p$, $3*p$, ...$(p^{k-1}-1)*p$ y el cero.

- Ejemplos

(16) = {1,3,5,7,9,11,13,15} ocho elementos
- ∴ $\phi(16) = \phi(2^4) = 2^{4-1}(2-1) = 2^3*1 = 8$

$\phi(125) = \phi(5^3) = 5^{3-1}*(5-1) = 5^2*4 = 25*4 = 100$

Función ϕ(n) de Euler cuando n = p∗q

n = p∗q (con p y q primos)

$$\phi(n) = \phi(p*q) = \phi(p)*\phi(q) = (p-1)(q-1)$$

De los p∗q elementos del CCR, restaremos todos los múltiplos de p = 1∗p, 2∗p, ... (q - 1)∗p, todos los múltiplos de q = 1∗q, 2∗q, ... (p - 1)∗q y el cero.

$$\phi(p*q) = p*q - [(q-1) + (p-1) + 1] = p*q - q - p + 1$$

(p-1)(q-1)

Ejemplos de ϕ(n) cuando n = p∗q

- Ejemplos

(15) = {1,2,4,7,8,11,13,14} ocho elementos

- ∴ ϕ(15) = ϕ(3*5) = (3-1)(5-1) = 2*4 = 8

ϕ(143) = ϕ(11*13) = (11-1)(13-1) = 10∗12 = 120

- Es la base del sistema RSA .
- Uno de sus usos más típicos podemos encontrarlo en las comunicaciones seguras del entorno Internet mediante SSL, tanto para el intercambio de claves como en los formatos de certificados digitales X.509 para firma digital.

Función ϕ(n) de Euler para n genérico

$n = p_1^{e1} * p_2^{e2} * \ldots * p_t^{et}$ (p_i son primos)

$$\phi(n) = \prod_{i=1}^{t} p_i^{ei-1} (p_i - 1)$$

- Ejemplos
  - (20) = {1, 3, 7, 9, 11, 13, 17, 19} ocho elementos
  - ∴ $\phi(20) = \phi(2^2 * 5) = 2^{2-1}(2-1)*5^{1-1}(5-1) = 2^1*1*1*4 = 8$

$\phi(360) = \phi(2^3 * 3^2 * 5) = 2^{3-1}(2-1)*3^{2-1}(3-1)*5^{1-1}(5-1) = 96$

Pequeño teorema de Fermat

- El **teorema de Fermat** se formula de la siguiente manera:
  - Si p es un número primo, entonces, para cada número natural a se tiene $a^p \equiv a \ (mod\ p)$.
- El teorema suele ser presentado de esta otra forma:
  - Si p es un número primo, entonces, para cada número natural a coprimo con p , $a^{p-1} \equiv 1 \ (mod\ p)$.
- Es decir, si se eleva un número a a la p-ésima potencia y al resultado se le resta a, lo que queda es divisible por p.
- Se aplica al problema de la primalidad y en criptografía.
  - Se comprueba si n (número que se quiere saber si es primo) es divisor del número $2^{n-1} - 1$.

Pequeño teorema de Fermat

Si el cuerpo de trabajo es un primo p: mcd (a, p) = 1 $\Rightarrow$ $a^{\phi(p)} \bmod p = 1$

Entonces $a * x \bmod p = 1$ y $a^{\phi(n)} \bmod p = 1$

Además, en este caso $\phi(p) = p-1$ por lo que igualando las dos ecuaciones de arriba tenemos:

$\therefore$ $a^{\phi(p)} * a^{-1} \bmod p = x \bmod p$

$\therefore$ $x = a^{p-2} \bmod p$

Luego x será el inverso de a en el primo p.

Teorema de Fermat (cont.)

- Ejemplo

$$7^{222} \bmod 11$$

$$7^{10} \equiv 1 (\bmod 11)$$

$$(7^{10})^k \equiv 1 (\bmod 11), k \in Z^+$$

$$7^{222} = 7^{22*10+2} = (7^{10})^{22} 7^2 \equiv (1)^{22} * 49 \equiv 5 (\bmod 11)$$

$$7^{222} \bmod 11 = 5$$

Teorema de Fermat (cont.)

- Sea *b* un número entero positivo. Si *n* es un número entero positivo compuesto, y $b^{n-1} \equiv 1 \pmod{n}$, entonces *n* se llama un **pseudoprimo** a la base *b*.

- El número 341 es psedoprimo a la base 2.

$$341 = 11 * 31$$

$$2^{340} \equiv 1 (\mathrm{mod}\, 341)$$

Teorema de Fermat (cont.)

- Un número entero compuesto *n* que satisface la congruencia $b^{n-1} \equiv 1 \pmod{n}$ para todos los enteros positivos *b* con *mcd*(*b*, *n*) = 1 se llama un número de *Carmichael*.

$$561 = 3 * 11 * 17$$

$$mcd(b,561) = 1$$

$$mcd(b,3) = mcd(b,11) = mcd(b,17) = 1$$

$$b^2 \equiv 1 (\mathrm{mod}\, 3), b^{10} \equiv 1 (\mathrm{mod}\, 11), b^{16} \equiv 1 (\mathrm{mod}\, 17)$$

$$b^{560} = (b^2)^{280} \equiv 1 (\mathrm{mod}\, 3)$$

$$b^{560} = (b^{10})^{56} \equiv 1 (\mathrm{mod}\, 11)$$

$$b^{560} = (b^{16})^{35} \equiv 1 (\mathrm{mod}\, 17)$$

$$b^{560} = 1 (\mathrm{mod}\, 561)$$

Teorema de Euler

- El **teorema de Euler**, también conocido como **teorema de Euler-Fermat**, es una generalización del teorema de Fermat, y como tal afirma una proposición sobre divisibilidad de números.
- El teorema establece que:
  - Si a y n son enteros primos relativos, entonces n divide al entero $a^{\varphi(n)} - 1$.
- Sin embargo, es más común encontrarlo con notación moderna en la siguiente forma:
  - Si a y n son enteros primos relativos, entonces $a^{\varphi(n)} \equiv 1 \pmod{n}$, donde $\varphi(n)$ es la **función φ de Euler**.

Teorema de Euler

Si mcd (a,n) = 1 $\Rightarrow$ $a^{\phi(n)} \bmod n = 1$

igualando $a*x \bmod n = 1$ y $a^{\phi(n)} \bmod n = 1$

$\therefore \quad a^{\phi(n)} * a^{-1} \bmod n = x \bmod n$

$\therefore \quad x = a^{\phi(n)-1} \bmod n$

El valor x será el inverso de a en el cuerpo n

Nota: Observe que se ha *dividido* por a en el cálculo anterior. Esto se puede hacer porque mcd (a, n) = 1 y por lo tanto hay un único valor inverso en el cuerpo n que lo permite.

Cálculo de inversos con Teorema Euler

- Ejemplo

  - ¿Cuál es el inverso de 4 en módulo 9? $\Rightarrow$ inv (4, 9)
  - Pregunta: ¿Existe a $*$ x mod n = 4 $*$ x mod 9 = 1?
  - Como mcd (4, 9) = 1 $\Rightarrow$ Sí ... aunque 4 y 9 no sean primos.
  - $\phi(9) = 6 \ \therefore \ x = 4^{6-1} \bmod 9 = 7 \Rightarrow 7*4 = 28 \bmod 9 = 1$
  - Resulta obvio que: inv (4, 9) = 7 e inv (7, 9) = 4

Teorema de Euler para n = p*q

Si el factor a es primo relativo con n y el valor n es el producto de 2 primos, seguirá cumpliéndose el Teorema de Euler también en dichos primos.

Por ejemplo:

Si $n = p*q \Rightarrow \phi(n) = (p-1)(q-1)$

$\forall$ a | mcd {a, (p,q)} = 1

se cumple que:

$a^{\phi(n)} \bmod p = 1$

$a^{\phi(n)} \bmod q = 1$

Ejemplo Teorema de Euler para n = p*q

- Sea n = p∗q = 7∗11 = 77
- $\phi(n) = (p - 1)(q - 1) = (7 - 1)(11 - 1) = 6*10 = 60$
- Si k = 1, 2, 3, ...
- Para a = k∗7 $a^{\phi(n)} \bmod n = k*7^{60} \bmod 77 = 56$
- Para a = k∗1 $a^{\phi(n)} \bmod n = k*11^{60} \bmod 77 = 22$
- Para ∀ a ≠ k∗7, k∗11 $a^{\phi(n)} \bmod n = a^{60} \bmod 77 = 1$
- Y se cumple también que:
- Para ∀ a ≠ k∗7, k∗11 $a^{\phi(n)} \bmod p = a^{60} \bmod 7 = 1$
  $a^{\phi(n)} \bmod q = a^{60} \bmod 11 = 1$
- En caso contrario: $a^{\phi(n)} \bmod p = 0$
  $a^{\phi(n)} \bmod q = 0$

Teorema de Fermat y Teorema de Euler

- La función φ de Euler se describe como:
  - Si *n* es un número entero, la cantidad de enteros entre 1 y *n* que son primos relativos con *n* se denota como φ(*n*):

Valor de *n*	Coprimos con *n* entre 1 y *n*	Función φ(*n*)
1	1	1
2	1	1
3	1,2	2
4	1,3	2
5	1,2,3,4	4
6	1,5	2
7	1,2,3,4,5,6	6
8	1,3,5,7	4
9	1,2,4,5,7,8	6
10	1,3,7,9	4

φ(n)	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9
0+		1	1	2	2	4	2	6	4	6
10+	4	10	4	12	6	8	8	16	6	18
20+	8	12	10	22	8	20	12	18	12	28
30+	8	30	16	20	16	24	12	36	18	24
40+	16	40	12	42	20	24	22	46	16	42
50+	20	32	24	52	18	40	24	36	28	58
60+	16	60	30	36	32	48	20	66	32	44
70+	24	70	24	72	36	40	36	60	24	78
80+	32	54	40	82	24	64	42	56	40	88
90+	24	72	44	60	46	72	32	96	42	60

46

Teorema de Fermat y Teorema de Euler

- Tal función es multiplicativa: si m y n son primos relativos, entonces $\varphi(mn)=\varphi(m)\varphi(n)$.
  - Ejemplo: $\varphi(30) = \varphi(6)\varphi(5) = 2 \cdot 4 = 8$
- Las aplicaciones son numerosas:
  - En criptografía es muy utilizado.
  - En la resolución de ecuaciones de congruencia.
  - En matemáticas puras, sobretodo, relacionadas con el problema de la primalidad.
    - Si n es primo la congruencia se cumplirá siempre, en caso contrario n es compuesto.
  - En el análisis de la descomposición en producto de factores primos de ciertos enteros, en la divisibilidad.

47

Teorema de Fermat y Teorema de Euler

- Por ejemplo, se desea encontrar todos los números x que satisfacen $5x \equiv 2 \pmod{12}$, todos los números x tales que 12 divida a $5x - 2$.
- El teorema de Euler dice que $5^{\varphi(12)} = 5^4 \equiv 1 \pmod{12}$ por lo que, multiplicando ambos lados de la ecuación por 5^3:
  - $5^3 \cdot 5x \equiv (5^3 \cdot 2 = 250) \equiv 10 \pmod{12}$
  - $5^4 x \equiv 10 \pmod{12}$
  - $x \equiv 10 \pmod{12}$

48

Teorema de Fermat y Teorema de Euler

- Entonces, la conclusión es que, cualquier número que al dividirse por 12 tenga residuo 10, será una solución de la ecuación.
- Se puede verificar con un ejemplo.
  - Si se divide 34 entre 12, el residuo es 10, por lo que $x = 34$ debe funcionar como solución.
  - Para verificarlo, se divide $34 \cdot 5 = 170$ entre 12, obtenemos un cociente 14 y un residuo 2, como se esperaba.

49

¿Qué hacemos si no se conoce ϕ(n)?

Calcular a^i mod n cuando los valores de i y a son grandes, se hace tedioso pues hay que utilizar la propiedad de la reducibilidad repetidas veces.

Si no conocemos ϕ(n) o no queremos usar los teoremas de Euler o Fermat, siempre podremos encontrar el inverso de a en el cuerpo n usando el

Algoritmo Extendido de Euclides

Teorema de Wilson

Teorema: p es primo si, y solo si

$$(p-1)! \equiv -1 \pmod{p}$$

Podemos considerar;

Sí p no es primo, asumiendo $p >= 5$, (para $p=4$, $3! \equiv 2 \pmod 4$)

Entonces $p=qr$ para algún $2 <= q < p$ y $2 <= r < p$.

Si $q \neq r$, entonces q y r aparecerán en $(p-1)!$,
por lo que $(p-1)! \equiv 0 \pmod p$.

Si $q = r$, entonces $p = q^2 > 2q$ (al asumir $p > 5$ y $q > 2$).
entonces q y 2q están en $(p-1)!$,
y por lo tanto $(p-1)! \equiv 0 \pmod p$.

Teorema de Wilson

Teorema: p es primo si, y solo si

$$(p-1)! \equiv -1 \pmod{p}$$

Para demostrarlo de otra forma utilizaremos el lema.

Lema. Si p es un número primo,
$x^2 \equiv 1 \pmod p$ si y solo si $x \equiv 1 \pmod p$ or $x \equiv -1 \pmod p$

Prueba. $x^2 \equiv 1 \pmod p$
si $p \mid x^2 - 1$
si $p \mid (x - 1)(x + 1)$
si $p \mid (x - 1)$ or $p \mid (x+1)$
si $x \equiv 1 \pmod p$ o $x \equiv -1 \pmod p$

Lema: p primo y $p \mid a \cdot b$ si $p \mid a$ o $p \mid b$.

Teorema de Wilson

Teorema: p es primo si, y solo si

$$(p-1)! \equiv -1 \pmod{p}$$

Considerando un ejemplo concreto.

$10!$
$\equiv 1\cdot2\cdot3\cdot4\cdot5\cdot6\cdot7\cdot8\cdot9\cdot10 \bmod 11$
$\equiv 1\cdot10\cdot(2\cdot6)\cdot(3\cdot4)\cdot(5\cdot9)\cdot(7\cdot8) \bmod 11$
$\equiv 1\cdot-1\cdot(1)\cdot(1)\cdot(1)\cdot(1) \bmod 11$
$\equiv -1 \bmod 11$

Además de 1 y 10, los números restantes se emparejan en inverso multiplicativo!

Teorema de Wilson

Teorema: p es primo si, y solo si

$$(p-1)! \equiv -1 \pmod{p}$$

Prueba. Como p es primo, todo número desde 1 a p-1 tiene inverso multiplicativo.

Por el Lema, todo número $2 <= k <= p-2$ tiene un inverso k' con $k \neq k'$.

Como p es impar, los números desde 2 a p-2 ` pueden agruparse en pares $(a_1,b_1),(a_2,b_2),\ldots,(a_{(p-3)/2},b_{(p-3)/2})$ así que $a_i b_i \equiv 1 \pmod{p}$

Por lo tanto,
$$\begin{aligned}(p-1)! &\equiv 1\cdot(p-1)\cdot2\cdot3\cdots\cdot(p-3)\cdot(p-2) \pmod{p}\\ &\equiv 1\cdot(p-1)\cdot(a_1b_1)\cdot(a_2b_2)\cdots\cdot(a_{(p-3)/2}b_{(p-3)/2}) \pmod{p}\\ &\equiv 1\cdot(-1)\cdot(1)\cdot(1)\cdots\cdot(1) \pmod{p}\\ &\equiv -1 \pmod{p}\end{aligned}$$

Referencias

- Ramírez Benavides, Kryscia Daviana. “Matemática Discreta”
- Ramió Aguirre, Jorge. “Seguridad Informática y Criptografía”
- Caballero Roldán, Rafael; Hortalá González, Teresa; Martí Oliet, Narciso; Nieva Soto, Susana; Pareja Lora, Antonio & Rodríguez Artalejo, Mario. “Matemática Discreta para Informáticos”. Pearson Prentice Hall, Madrid. Primera Edición, 2007.
- Murillo, Manuel. “Introducción a la Matemática Discreta”. 2da edición, Editorial Tecnológica de Costa Rica. Cartago, 2007.

55