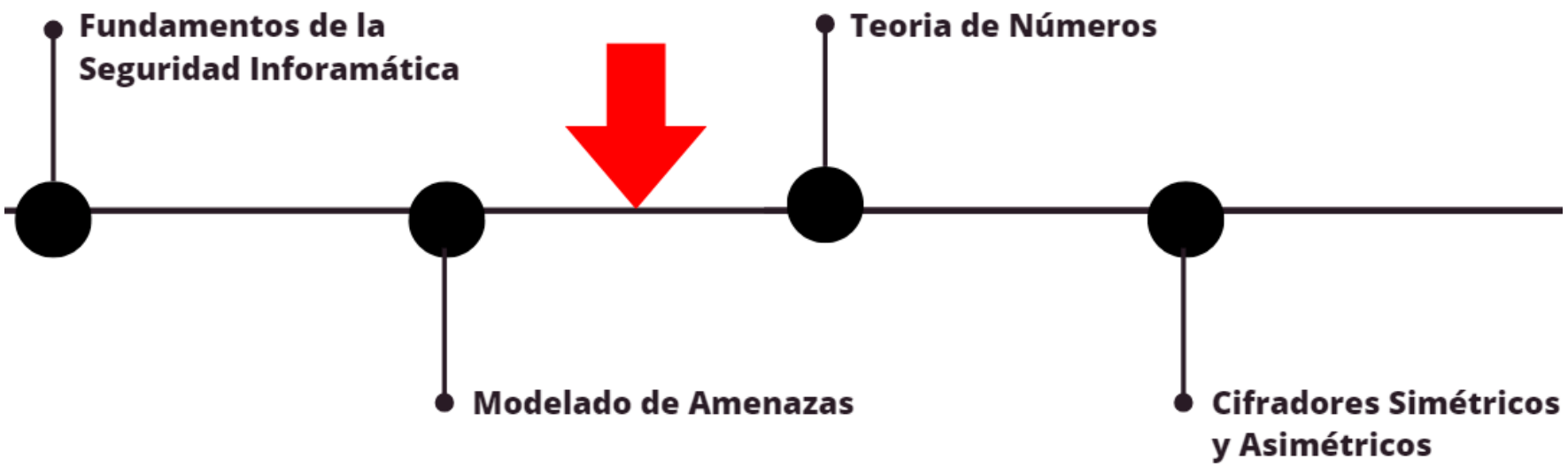
Criptografía y Seguridad Informática

Teoría de números

Agenda


Fundamentos de la Seguridad Inforamática
Modelado de Amenazas
Teoria de Números
Cifradores Simétricos y Asimétricos

Agenda

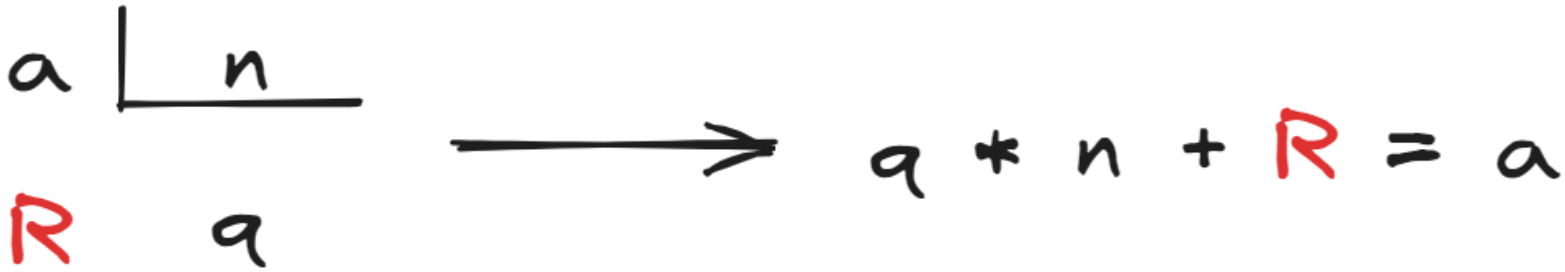
- Aritmética Modular
- Estructuras Algebraicas: Campos finitos
- Primos y primos relativos el conjunto Z^*
- Algoritmo de Euclides para el cálculo de MCD
- Existencia de la inversa en Z^*
- La función de Euler y el teorema de Euler y Fermat
- Logaritmo discreto
- Test de primalidad y generación de números primos

Aritmética Modular

Teoría de números

Aritmética Modular

Dado un entero positivo **n** y cualquier entero **a**, si se divide a **a** por **n**, se obtiene un cociente q y un residuo entero r que cumple con la siguiente relación:



Operaciones Modulares

- Resto modular
  - 17 mod 20 = 17
- Suma y resta modular
  - 45 + 33 mod 60 = 78 mod 60 = 18
  - 58 - 75 mod 50 = -17 mod 50 = 33
- Multiplicación modular
  - 127x39 mod 1.001 = 4.953 mod 1.001 = 949
- Potencia (exponenciación) modular
  - 98.717^5 mod 1.510 = 9.374.751.048.109.369.618.733.357 mod 1.510 = 377

Congruencias

- *Definición:*
  - *Sean dos números enteros a y b: se dice que a es congruente con b en el módulo o cuerpo n (Z_n) si y sólo si existe algún entero k que divide de forma exacta la diferencia (a - b) .*
  - *Se dice que dos enteros a y b son congruentes modulo n, si se cumple*

$$a \equiv b \bmod n \longrightarrow a - b = k * n$$

$$a = k * n + b$$

$$a = b \bmod n$$

Ejemplo congruencia

$$73 \equiv 4 (\mathrm{mod} 23); \quad 21 \equiv -9 (\mathrm{mod} 10)$$

Ejemplo en módulo 7

```
...
-21  -20  -19  -18  -17  -16  -15
-14  -13  -12  -11  -10   -9   -8
 -7   -6   -5   -4   -3   -2   -1
  0    1    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
...
```

Los números de una misma columna son congruentes

Propiedades de la congruencia en Zn

Propiedad Reflexiva:

$$a = a \bmod n \quad \forall\, a \in Z$$

Propiedad Simétrica:

$$a = b \bmod n \longrightarrow b = a \bmod n \quad \forall\, a, b \in Z$$

Propiedad Transitiva:

$$\text{Si } a = b \bmod n \quad \text{y} \quad b = c \bmod n$$

$$\longrightarrow a = c \bmod n \quad \forall\, a,b,c \in Z$$

Divisor

Se dice que un no-cero **b** divide **a** si:
a = mb para algún m, donde a, b y m son enteros.

Esto es, b divide a si no existe ningún residuo en la división.

La notación b | a es usada para indicar que b divide a.
También, si b|a, se dice que b es un divisor de a.

Ejemplo divisores

Los divisores positivos de 24 son $1, 2, 3, 4, 6, 8, 12$ y 24.

Reducibilidad

Cuando sumas dos números a y b y luego tomas el resultado modulo n, puedes reducir la operación tomando el módulo de cada número previamente

1. $[(a \bmod n) + (b \bmod n)] mod n = (a + b) \bmod n.$
2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n.$
3. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n.$

Ejemplo

$$\begin{aligned}[(11 \bmod 8) + (15 \bmod 8)] \bmod 8 &= [(3) + (7)] \bmod 8 \\ &= 10 \bmod 8 \\ &= 2 \bmod 8\end{aligned}$$

Reducibilidad

Cuando sumas dos números a y b y luego tomas el resultado modulo n, puedes reducir la operación tomando el módulo de cada número previamente

1. $[(a \bmod n) + (b \bmod n)] mod n = (a + b) \bmod n.$
2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n.$
3. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n.$

Ejemplo

$$\begin{aligned}[(11 \bmod 8) + (15 \bmod 8)] \bmod 8 &= [(3) + (7)] \bmod 8 \\ &= 10 \bmod 8 \\ &= 2 \bmod 8\end{aligned}$$

Estructuras Algebraicas

Teoría de números

Grupo Abeliano

Conjunto de números con una operación binaria (suma), que satisface las siguientes propiedades

- (a1) Cerrado:

  si a y b pertenecen a Z_n => a+b mod n también
- (a2) Propiedad asociativa

  a + (b + c) mod n = (a + b) + c mod n
- (a3) Identidad

  a + 0 mod n = 0 + a mod n = a mod n
- (a4) Inversa aditiva

  a + (-a) mod n = 0 (3 + 4) mod 7 = 0
- (a5) Conmutativa

  a + b mod n =b + a mod n

Anillo

Conjunto de números con dos operaciones (S,+,.) (suma y multiplicación) que satisface las siguientes propiedades:

- (a1) Grupo abeliano con respecto a la suma

- (a2) Multiplicación:
  - (m1) cerrada
    - Si a ^ b ε S => a*b ε S
  - (m2) Asociativa
    - a.(b.c) mod n = (a.b).c mod n
  - (m3) distributiva respecto de la suma:
    - a * (b+c) mod n = ((a * b) + (a * c)) mod n

Dominio

Anillo Conmutativo

- (m4) Si la operación de multiplicación es conmutativa

  $a * b \bmod n = b * a \bmod n$

Dominio

- (m5) Identidad multiplicación

  $a * 1 \bmod n = 1 * a \bmod n = a \bmod n$

- (m6) No hay divisores nulos

  Si $a.b = 0 \Rightarrow a=0$ o $b=0$

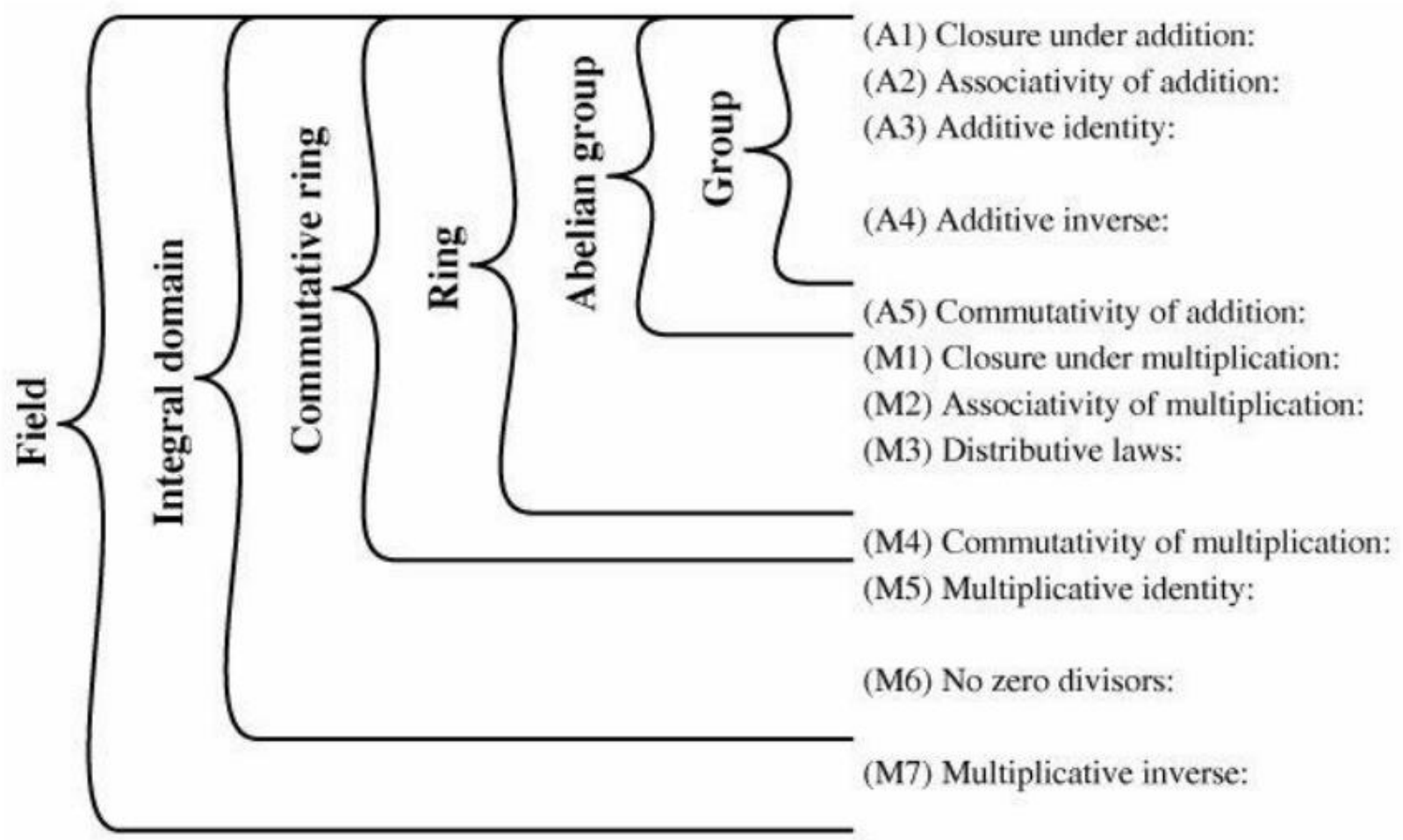
Campo Finito

Un conjunto de números con dos operaciones (S,+,.) (suma y multiplicación) que satisface las siguientes propiedades :

- Dominio
- (m7) Inversa multiplicativa

  - Si $a \varepsilon S \wedge a \neq 0, a^{-1} \varepsilon S / a.\ a^{-1} = 1$
  - $a * (a^{-1}) \bmod n = 1$

Resumen



Cryptography and Network Security, Principles and Practices (William Stallings)

Resumen

Si tomo un conjunto de números enteros, defino las operaciones suma y multiplicación en forma modular, y logro que para cualquier elemento exista inversa multiplicativa, entonces tengo un campo finito!

Primos y Primos Relativos

Teoría de números

Números primos y números compuestos

- **Números Primos**: Un número primo es un número entero mayor que 1 que solo tiene dos divisores distintos: 1 y él mismo.
  => 19 es primo

- **Números Compuestos**: Compuesto si esta representado como la multiplicación de dos o más primos
  => 273 es compuesto ya que es igual a 3 * 7 * 13

- **Coprimos**: Dos números son primos relativos o coprimos si en su descomposición en números primos no tienen ningún factor en común => 6 y 25 son comprimos ya que 6 = 2*3 y 25 = 5*5

  - **Si a y b coprimos, mcd (a,b) = 1**
  - **Si tomamos cualquier número primo p, todos los números enteros anteriores a p son coprimos con p**

Máximo común divisor (GCD)

- Se utiliza la notación **gcd(a, b)** para designar el máximo común divisor de a y b.
- El entero c es el máximo común divisor de a y b si
  - c es el divisor de a y de b
  - Cualquier divisor de a y b es un divisor de c

- Ejemplo: GCD(60,24) = 12

Primo Relativo

- Dos enteros a y b son primos relativos si gcd(a,b) = 1
- Dado que GCD(8,15) = 1 => son primos relativos

Algoritmo de Euclides

- Método para encontrar el máximo común divisor (gcd)

```
GCD(a,b) = GCD(b, a mod b)
```

- **Algoritmo**

1. $A \leftarrow a;\ B \leftarrow b$
2. Si $B = 0$ regresa $A = gcd$
3. $R = A \bmod B$
4. $A \leftarrow B$
5. $B \leftarrow R$
6. Ir a paso 2

GCD (36, 24)

(1) A = 36 y B = 24
(2) ¿B = 0? No
(3) R = 36 mod 24 = 12
(4 y 5) A = 24 , B = 12
(2) ¿B = 0? No
(3) R = 24 mod 12
(4 y 5) A = 12, B = 0
(2) ¿B = 0? Si => GCD = 12

Algoritmo de Euclides

Manera eficiente de calcular GCD(a,b)

- `GCD(a,b) = GCD(b, a mod b)`

Pseudo-Código

- GCD (a,b)
  - `A=a, B=b`
  - `while B>0`
    - `R = A mod B`
    - `A = B, B = R`
  - `return A`

Conjunto Clase de Residuos (CCR O Zn)

CCR o Zn : Conjunto de números enteros que resultan de la división de cualquier entero por un número fijo **n.**

$$Z_n = \{0, 1, \ldots, (n-1)\}$$

Clase de Equivalencia: Consiste en todos los enteros que producen el mismo residuo cuando se dividen por n.

Ejemplo: n = 4 => Zn = {0,1,2,3}

[0] = {..., −16, −12, −8, −4, 0, 4, 8, 12, 16, ...}

[1] = {..., −15, −11, −7, −3, 1, 5, 9, 13, 17, ...}

[2] = {..., −14, −10, −6, −2, 2, 6, 10, 14, 18, ...}

Conjunto reducido de residuos

Conjunto reducido de residuos Z*: El conjunto de los primos relativos a n

Ejemplo:

- si n=6 => 6=2*3
- Z* = (1,5)

- Si n primo, todos los anteriores son coprimos
- Zn = Z* con n primo

Aritmética Modular

- Las operaciones modulares en criptografía se realizarán dentro de un módulo de cifra, cuyo número puede ser primo o compuesto

- Entonces si tomamos: $Z_n = \{0, 1, \ldots, n-1\}$

  - Anillo conmutativo para la suma
  - Campo finito para N primo

Inversa en Zn

Si $a * x = 1 \bmod n$ se dice que x es el inverso multiplicativo de a en Z_n y se denotará por a^{-1}.

No siempre existen por ejemplo si n=10 no existe inverso ya que 5*x=1 mod 10 no tiene solución

No existencia de inversos

$(A * B) \bmod 10$

	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9
2	2	4	6	8	0	2	4	6	8
3	3	6	9	2	5	8	1	4	7
4	4	8	2	6	0	4	8	2	6
5	5	0	5	0	5	0	5	0	5
6	6	2	8	4	0	6	2	8	4
7	7	4	1	8	5	2	9	6	3
8	8	6	4	2	0	8	6	4	2
9	9	8	7	6	5	4	3	2	1

Para módulo 10 sólo encontramos inversos multiplicativos en los restos 3, 7 y 9, puesto que los demás restos tienen factores 2 y 5 en común con el módulo.

Existencia de la Inversa en Z*

(1) Multiplicación cerrada en Z*: Si multiplico dos elementos de Z* tendré otro elemento en Z*

Si a y ri esta en Z* y calculamos (a * ri) mod n = rj ⟶ rj esta en Z*
(si no fuera primo relativo forzaría a que a o ri tampoco lo sean)

- Supongo RJ no es primo relativo entonces tendrá un factor K con N
- => $R_J=K*R_J'$ y $N=K*N'$ (los dos tendran el factor K)
- sabemos que $a*ri= qN + rj$
- Reemplazando $a*ri= q\ K\ N' + K * rj' =$

  $a*ri= K(qN'+rj')$
- Uno de los dos debería tener de factor a K ➔ Absurdo

.

Existencia de la Inversa en Z*

(2) Si multiplico por dos números diferentes de Z* me dan diferentes

Si mcd (a, n) = 1 => a * i ≠ a * j mod n (i,j Primos Relativos)

Si suponemos lo contrario => n | (a*i - a*j)

=> n | a(i-j)

=> n|(i-j)

=> i ≡ j mod n (CONTRADICCION)

De la propiedad del slide anterior y esta:

- ***Al multiplicar a por el set reducido de elementos va a dar una permutación de los elementos y se generara el set completo*.**
- ***Obligatoriamente uno de ellos dará el 1 y será su inversa***

Generación del Set Completo

N=50 => Z^* = (1 , 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39, 41, 43, 47, 49)

	1	3	7	9	11	13	17	19	21	23	27	29	31	33	37	39	41	43	47	49
1	1	3	7	9	11	13	17	19	21	23	27	29	31	33	37	39	41	43	47	49
3	3	9	21	27	33	39	1	7	13	19	31	37	43	49	11	17	23	29	41	47
7	7	21	49	13	27	41	19	33	47	11	39	3	17	31	9	23	37	1	29	43
9	9	27	13	31	49	17	3	21	39	7	43	11	29	47	33	1	19	37	23	41
11	11	33	27	49	21	43	37	9	31	3	47	19	41	13	7	29	1	23	17	39
13	13	39	41	17	43	19	21	47	23	49	1	27	3	29	31	7	33	9	11	37
17	17	1	19	3	37	21	39	23	7	41	9	43	27	11	29	13	47	31	49	33
19	19	7	33	21	9	47	23	11	49	37	13	1	39	27	3	41	29	17	43	31
21	21	13	47	39	31	23	7	49	41	33	17	9	1	43	27	19	11	3	37	29
23	23	19	11	7	3	49	41	37	33	29	21	17	13	9	1	47	43	39	31	27
27	**27**	**31**	**39**	**43**	**47**	**1**	**9**	**13**	**17**	**21**	**29**	**33**	**37**	**41**	**49**	**3**	**7**	**11**	**19**	**23**
29	29	37	3	11	19	27	43	1	9	17	33	41	49	7	23	31	39	47	13	21
31	31	43	17	29	41	3	27	39	1	13	37	49	11	23	47	9	21	33	7	19
33	33	49	31	47	13	29	11	27	43	9	41	7	23	39	21	37	3	19	1	17
37	37	11	9	33	7	31	29	3	27	1	49	23	47	21	19	43	17	41	39	13
39	39	17	23	1	29	7	13	41	19	47	3	31	9	37	43	21	49	27	33	11
41	41	23	37	19	1	33	47	29	11	43	7	39	21	3	17	49	31	13	27	9
43	43	29	1	37	23	9	31	17	3	39	11	47	33	19	41	27	13	49	21	7
47	47	41	29	23	17	11	49	43	37	31	19	13	7	1	39	33	27	21	9	3
49	49	47	43	41	39	37	33	31	29	27	23	21	19	17	13	11	9	7	3	1

Función de Euler Φ(n)

- Se define Φ(n) como la cantidad de primos relativos a n
- Si n primo => Φ(n) = n - 1
- Si n multiplicación de primos
  - n = p*q => Φ(n) =(p-1)*(q-1)
- $\Phi(n) = \pi_{i=1}^{n} \{ p_i^{ei-1} (p_i - 1) \}$ → Queremos calcular Φ(24)

$24 = 2 * 3$
$p1=2,\ e1=3,\ p2=3,\ e2=1$

$\Phi(24) = (2^{3-1} * (2-1)) * (3^{1-1} * (3-1)) = 8$

Función Φ(n) de Euler cuando n = p * q

- n = p*q (con p y q primos)

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

- 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.

- $\Phi(p*q) = p*q - [(q-1) + (p-1) + 1] = \underbrace{p*q - q - p + 1}_{(p-1)(q-1)}$

Función Φ(n) de Euler cuando n = p * q

- **Ejemplo**

$$p = 3,\ q = 5$$

$$n = p * q = 15 = 3 * 5$$

$$Z* = \{1,2,4,7,8,11,13,14\}$$

Teorema de Euler

$$a^{\Phi(n)} \equiv 1 \bmod(n)$$

Dem: Si multiplico entre si todos los elementos de Z* y luego a cada elemento lo multiplico por a.

$$\pi\ r_i =_n \pi\ (a^* r_i) =_n a^{\Phi(n)} \pi\ r_i$$

Al ser una permutación de los elementos de ri la primer igualdad es valida.

$$\pi\ r_i =_n a^{\Phi(n)} \pi\ r_i \rightarrow {}_A\Phi(n) =_n 1$$

Teorema de Fermat

Si n primo: $a^{p-1} \equiv 1 \bmod p$

DEM: Se deduce del teorema de euler

Inversa usando Teorema de Euler

- $a^{\Phi(n)} \equiv a * a^{\Phi(n)-1} \equiv 1 \bmod(n)$
- $a^{-1} \equiv a^{\Phi(n)-1} \bmod(n)$
- Ejemplo:

Inverso de 4 mod 15:

$4 * x \bmod 15 = 1$

$\Phi(15) = (p-1)*(q-1) = (3-1) * (5-1) = 12$

$a^{-1} = a^{\Phi(n)-1} \bmod 14 = 4^{12-1} \bmod 15 = 4$

$4*4 = 16 \bmod 15 = 1$

Inversa usando Euclides Extendido

El algoritmo de Euclides extendido es una extensión del algoritmo de Euclides estándar que se utiliza para encontrar el inverso modular de un número.

Algoritmo de Euclides extendido:

```
Inverse of b mod m => EXTENDED EUCLID(m, b)
1.  (A1, A2, A3)=(1, 0, m);
    (B1, B2, B3)=(0, 1, b)
2. if B3 = 0
    return A3 = gcd(m, b); no inverse
3. if B3 = 1
    return B3 = gcd(m, b); B2 = b^-1 mod m
4. Q = A3 div B3
5. (T1, T2, T3)=(A1 - Q B1, A2 - Q B2, A3 - Q B3)
6. (A1, A2, A3)=(B1, B2, B3)
7. (B1, B2, B3)=(T1, T2, T3)
8. goto 2
```

Inverse of 550 in GF(1759)

Q	A1	A2	A3	B1	B2	B3
—	1	0	1759	0	1	550
3	0	1	550	1	-3	109
5	1	-3	109	-5	16	5
21	-5	16	5	106	-339	4
1	106	-339	4	-111	355	1

Inverse

Inversas: Euclides Extendido

La idea es mantener invariante a

$m*B1 + b*B2 = B3$ y a

$m*A1 + b*A2 = A3$

En la ultima linea $m* B1 + b*B2 =1$

➔ $b*B2 = 1-mB1$

➔ $b*B2 = 1 \bmod(m)$ Es decir B2 es la inversa de b

La exponenciación en la cifra asimétrica

- Una de las aplicaciones más interesantes de la matemática discreta en criptografía es la cifra asimétrica en la que la operación básica es una exponenciación A^B mod n, en donde n es un primo grande o un producto de primos grandes.

- Esta operación A^B mod n se realizará para el intercambio de clave y en la firma digital.

- ¿Cómo hacer estos cálculos de forma rápida y eficiente, sin tener que aplicar reducibilidad?

Un método de exponenciación rápida

- *En A^B mod n se representa el exponente B en binario.*

Vamos a calcular $x = 12^{37} \bmod 221$

$$12^{37} = 12^{100101_{(2)}}$$

- *Se calculan los productos A^{2^j} con j = 0 hasta n-1, siendo n el número de bits que representan el valor B en binario.*

$n = 5$

$12^{2^0} = 12$, $12^{2^1} = 144$, $12^{2^2} = 183$, $12^{2^3} = 118$, $12^{2^4} = 1$, $12^{2^5} = 1$

Un método de exponenciación rápida

- *Sólo se toman en cuenta los productos en los que en la posición j del valor B en binario aparece un 1.*

$12^{37} = 12^{100101_{(2)}}$ ⟶ Solo tomo en cuenta los productos de la posicion 0,2 y 5

$12^{37} = 12^{2^0} * 12^{2^2} * 12^{2^5} \bmod 221 = 12 * 183 * 1 \bmod 221 = 207$

- *La exponenciación pasa de ser un algoritmo O(n) a un algoritmo O(log n)*

Un método de exponenciación rápida

- *Algoritmo:*

```
int pot(int a, int n) {
    if (n == 0) return 1;
    int x = pot(a, n/2);
    if (n % 2 == 0) return x*x;
    return x*x*a;
}
```

Raíz primitiva o generador de un primo

Un generador o raíz primitiva de un número primo p es aquel valor que, elevado a todos los restos del cuerpo reducido módulo n, genera todo el cuerpo.

Así, g es un generador si: $\forall \quad 1 \leq a \leq p-1$

$g^a \bmod p = b$ (con $1 \leq b \leq p-1$, todos los $b \neq$)

Sea p = 3 $\longrightarrow$CCR = {1,2} (el cero no es solución)

Resto 1: no generará nada porque $1^k \bmod p = 1$

Resto 2: $2^1 \bmod 3 = 2$; $2^2 \bmod 3 = 1$

Luego el 2 es un generador del cuerpo n = 3

Ejemplo raíz primitiva

Si n = 14 Z^*_{14}

= { 1,3,5,9,11,13}

$$5^0 = 1$$
$$5^1 = 5$$
$$5^2 = 25 \equiv 11 \pmod{14}$$
$$5^3 = 5^2 \times 5 \equiv 11 \times 5 = 55 \equiv 13 \pmod{14}$$
$$5^4 = 5^3 \times 5 \equiv 13 \times 5 = 65 \equiv 9 \pmod{14}$$
$$5^5 = 5^4 \times 5 \equiv 9 \times 5 = 45 \equiv 3 \pmod{14}$$

Obtenemos todos los elementos de Z^*_{14} como potencias de 5

Logaritmo discreto

$$x = \log_g(y) \iff g^x = y$$

- *Dado un par de enteros α y* p *se pide encontrar un entero x de forma tal que x = $\log_\alpha$* p *mod p.*
- *Si el valor p es muy grande, el Problema del Logaritmo Discreto PLD es computacionalmente intratable.*
- *No obstante, el caso inverso, dado dos números α y x, encontrar*
- p = α^x *mod p es un problema polinomial.*
- *Este problema se usará, entre otros, en la creación de las claves del sistema de cifra con clave pública ElGamal y en el protocolo de intercambio de clave de Diffie y Hellman.*

El problema de la factorización

- Dado n = p*q se pide encontrar estos factores.

- Por ejemplo, cuando el valor n = p*q es muy grande, el Problema de la Factorización de Números Grandes PFNG se vuelve computacionalmente intratable.

- No obstante, el caso inverso, dado dos números primos p y q, encontrar el resultado p*q = n, se trata de un problema de tipo polinomial.

- Se usa en RSA.

Test de primalidad

- Para números muy grandes, como los usados en RSA, que llegan a tener tamaños de 2048 bits
- no es viable en un tiempo razonable tratar de factorizar un número para saber si es o no primo.
- Test de Primalidad:
  - Dan un resultado probable sobre la primalidad de *p* con una probabilidad de error determinada.
  - mediante iteraciones sucesivas obtenemos mayor grado de certeza.

Test de primalidad de Miller–Rabin

(1) N impar, con $N = 2^s * r + 1$

(2) Se elige al azar un entero a con $1 < a < n$

(3) Si $a^r = 1$ o -1 mod n retorna probable primo y termina

(4) Sino, $a^{2^j * r}$ mod n para j = 0, ... , s-1
Si el resultado es -1 -> Probable primo y termina
Si el resutlado es 1 -> Compuesto y termina

(5) Si no se encontro evidencia de probable primo o compuesto, se asume compuesto.

Si se obtiene k veces la respuesta *probable primo*, entonces la probabilidad de error es inferior a $1/2^{2k}$ lo que lo hace *muy* fiable.

Test de primalidad de Miller–Rabin

Ejemplo

(1) $N = 1729$, $N = 2^6 * 27$ -> $s = 6$, $r = 27$

(2) Elijo $a = 671$ $(1 < a < 1729)$

(3) $671^{27} = 1084 \bmod 1729$

(4) $671^{27 * 2} = 1065 \bmod 1729$

(5) $671^{27 * (2)^2} = 1 \bmod 1729$

-> Es declarado compuesto y termina

Generación de números primos

- Generar un número aleatorio *p* de n bits.
- Poner a uno el bit más significativo (debe ser impar)
- Intentar dividir *p* por una tabla de primos precalculados. Los menores que 2000.
  - el 99.8 % de los números impares no primos es divisible por algún número primo menor que 2000.
- Ejecutar tests de primalidad para ver si es primo hasta el grado de certeza deseado
- Si el test falla, incrementar *p* en dos unidades y volver al paso 3.

¿Cuántos números primos hay?

Por el teorema de los números primos, se tiene que la probabilidad de encontrar números primos a medida que éstos se hacen más grandes es menor:

Números primos en el intervalo [2, x] = x / ln x

- *Primos entre 2 y 2^5 = 32 x/lnx = 32/3,46 = 9* *Probabilidad x sea primo: 30,00 %*
- *Primos entre 2 y 2^6 = 64 x/lnx = 64/4,16 = 15* *Probabilidad x sea primo: 24,00 %*
- *Primos entre 2 y 2^7 = 128* *x/lnx = 128/4,85 = 26* *Probabilidad x sea primo: 20,63 %*
- *Primos entre 2 y 2^8 = 256* *x/lnx = 256/5,54 = 46* *Probabilidad x sea primo: 18,11 %*
- *Primos entre 2 y 2^9 = 512* *x/lnx = 512/6,23 = 82* *Probabilidad x sea primo: 16,08 %*
- *Primos entre 2 y 2^{10} = 1.024* *x/lnx = 1.024/6,93 = 147* *Probabilidad x sea primo: 14,38 %*
- *Primos entre 2 y 2^{11} = 2.048* *x/lnx = 2.048/7,62 = 268* *Probabilidad x sea primo: 13,10 %*
- *Primos entre 2 y 2^{12} = 4.096* *x/lnx = 4.096/8,32 = 492* *Probabilidad x sea primo: 12,02 %*

http://www.criptored.upm.es/descarga/Class4cryptc4c2.1_Aritmetica_modular_restos_Euler.pdf