Tema 1: Fundamentos Matemáticos

- **Estructuras**: Sea a, b ∈ Z, Z tiene estructura de:
  - **Grupo (Z,+)** si cumple las siguientes propiedades:
    - Cierre, a+b sigue perteneciendo a Z
    - Asociativa, a+(b+c) =(a+b)+c
    - Identidad, a+0=0
    - Inverso, a+(-a)= 0
  - **Grupo Conmutativa o Abeliano** si ademas de las Grupo cumple:
    - Conmutativa, a+b=b=a
  - **Anillo (Z,+,*)** si cumple las de anillo y ademas para el producto:
    - Cierre
    - Asociativa
    - Identidad

    Esas 3: $(Z,\cdot)$ es semigrupo.
    - * es distributiva respecto +, a*(b+c)= (a*b)+(a*c)
  - **Anillo Conmutativo** si ademas de las de Anillo cumple la conmutativa.
  - **Anillo de División** si cumple las de anillo y ademas: Inverso, a*a^1=1
  - **Cuerpo**: Anillo de División Conmutativo.

- **Congruencias:** Sean a, b, n ∈ Z, a y b serán congruentes modulo n (a≡b mod n)
  - Si la diferencia entre a y b es un múltiplo de n. **a-b=n*k / k entero**
  - También si ambos dejan el mismo resto si los dividimos por n.
  - **Clase de congruencias de a modulo ([a]$_n$):** Conjunto de todos los números congruentes con a modulo n, se genera sumando y restando n. $[3]_{10}$ ={..., -17, -7, 3, 13, 23,...}
- **Reducción modulo n:** Se busca que a sea un valor entre 0 y n-1.
  - Restar/Sumar n hasta quedarse con el numero positivo mas bajo.
    - 16 mod 5=16-15 mod 5=1 mod 5
  - Dividir entre n, y quedarse con el resto. 16 mod 5= 1 mod 5

16 | 5
1 | 3

- **Conjunto Z_n:** Conjunto de clases de congruencia respecto al modulo n. Va desde 0 hasta n-1.
    - Z_7={0, 1, 2, 3, 4, 5, 6}
  - **Operación suma/resta/producto $+_n$/$-_n$ /$*_n$** : Siendo los términos respecto a mismo modulo, consiste en hacer la operación entre sus valores y el resultado modulo n.
  - $[2] +_5 [4] = (2+4) \bmod 5 = 6 \bmod 5 = 1 \bmod 5 = [1]$
  - **Principios fundamentales de la Aritmética Modular:**
    - (a + b) (mód. n) = (a(mód. n) + b(mód. n))(mód. n)
    - (a*b) (mód. n) =(a (mód. n) * b (mód. n)) (mód. n)
    - (a*(b+c)) (mód. n) =((a* b) (mód. n)+(a*c) (mód. n)) (mód. n)

$$(3 \cdot (8+4)) \bmod 5 =$$

$$((3 \cdot 8) \bmod 5 + (3 \cdot 4) \bmod 5) \bmod 5 =$$

$$(9 \bmod 5 + 12 \bmod 5) \bmod 5 =$$

$$(4+2) \bmod 5 = 6 \bmod 5 = 1 \bmod 5 = 1$$

- **Cálculo de Inversos:** El m.c.d de a y n debe ser 1, para que sean coprimos(el único divisor que tiene en común es el 1). **a^(-1)*a=1. a*x=1 mod n. x=a^(-1) mod n**
  - **Teorema de Fermat:** Si p es primo y mcd(a, p)=1, se cumple:

$a^{p-1} \text{ mód. } p = 1$ por lo tanto el inverso $\Rightarrow$ $\bar{a}^{-1} = a^{p-2} \text{ mód. } p$

$2x \bmod 7 = 1 \quad x = 2^{-1} \bmod 7 = 1$

mcd(2,7)=1, 7 primo $\quad x = 2^{7-2} \bmod 7 = 2^3 \cdot 2^2 \bmod 7 = 4 \bmod 7$; $x = 4 \bmod 7$ ($1 \cdot 4$)

  - **Teorema de Euler:** mcd(a, n)=1, aunque no tiene porque ser primo, se cumple:

$a^{\phi(n)} \text{ mod. } n = 1$ y para el inverso $\Rightarrow$ $a^{\phi(n)-1} \text{ mod. } n = \bar{a}^{-1}$

$3x \bmod 10$

mcd(3,10)=1, $10 = 5 \cdot 2$ no primo $\quad x = 3^{-1} \bmod 10 = 3^{\phi(10)-1} \bmod 10 = 3^3 \bmod 10$ ($27 - 2 \cdot 10 = 7$)

$\phi(10) = \phi(2)\phi(5) = 1 \cdot 4 = 4$

$x = 7 \bmod 10$

    - Indicador de Euler: Indicador del numero de elementos de Zn*

Para p primo $\phi(p) = p - 1$ $\quad \phi(p^x) = p^{x-1}(p-1)$ ↳ Por eso Fermat es a^{p-1}

Para p y q primos $\phi(p \cdot q) = \phi(p) \cdot \phi(q)$

$\phi(28) = \phi(2^2 \cdot 7) = \phi(2^2)\phi(7) = (2^1 \cdot 1) \cdot (6) = 12$

    - **Conjunto Zn*:** Conjunto de números que son coprimos con n.
      - $Z_{12}^* = \{1, 5, 7, 11\}$ $\varphi(12) = \varphi(2^2 * 3) = 2^1 * 1 * 2 = 4$
  - **Algoritmo de Euclides:** Permite hallar el mcd de dos números enteros positivos sin necesidad de factorizar los números. También permite hallar el inverso de un numero respecto a otro cuando el mcd de ambos es 1(coprimos), y despejar el 1.
    - Ejem: mcd de 1547 y 560, poner el mayor igualado al menor por un entero, mas resto.
    - 1547 = 2 · 560 + 427 (buscamos el multiplo de 560 mas cercano a 1547, $2 \cdot 560$ y resto 427)
    - 560 = 1 · 427 + 133
    - 427 = 3 · 133 + 28
    - 133 = 4 · 28 + 21
    - 28 = 1 · 21 + 7
    - 21 = 3 · 7 + 0 (El ultimo resto no nulo (0))
    - m.c.d.(1547,560) = 7 ≠1 no tiene inverso
    - Ejem: calculo de inverso de 23x mod 25, ir dejando el resto 1 mediante todas las ecuaciones y el inverso será el que acompaña al 23. $x = 23^{-1} \bmod 25$
    - 25=1·23+2 $\quad 1 = 23 - 11(25 - 23) = 12 \cdot 23 - 11 \cdot 25$
    - 23=11·2+1 $\quad 1 = 23 - 11 \cdot 2$ $\quad 1 = 12 \cdot 23 \bmod 25 - 0$ ($11 \cdot 25 \bmod 25$)
    - 11=11·1+0 $\quad 23^{-1} = 12 \bmod 25$
    - mcd(25, 23)= 1 Coprimos podemos hallar el inverso. $x = 12 \bmod 25$
  - **ax=b mod. n** debe cumplirse mcd(a,n)|b:
    - Si mcd(a, n)= 1, hay una solución. Se resuelve el inverso de a y se multiplica por b.
    - Si mcd(a, n)=m!=1, hay m soluciones. Se simplifica la expresión y se resuelve como el anterior, con la diferencia de que las soluciones serán con el modulo original y se harán crearan el resto de soluciones sumando el modulo del simplificado.
    - Otro método es con Ecuaciones diofánticas: ax+ny=b, simplificamos la expresión y damos valor a x e y, y operamos para que quede el =b simplificado. Se resta la expresión en la que hemos dado valor a x e y con la original simplificada. Dando valor a k, hallamos las soluciones x.

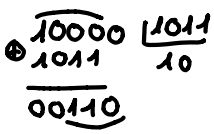
$x = 5k - 2$ $\quad 5 \cdot k = x + 2$ $\Rightarrow 3(x+2) = 5(y+1)$ (suma y resta)

Cuando se pueda se simplifica

- **Cuerpos de Galois CG(p):** Sea Zp={0, 1, 2,..., p-1} siendo p primo. Zp es un cuerpo finito denominado Cuerpo de Galois CG(p). Zp=CG(p)
  - Zp es un cuerpo respecto a la suma y la multiplicación.
  - Hay p elementos en GC(p).

- **Cuerpos de Galois CG(q^n):** Esta formado por los polinomios de grado n-1 o menor. Si al operar obtenemos un polinomio de grado n o mayor, se reduce modulo de un polinomio p(x), que nos lo dan y normalmente es: **p(x)=x^n+x+1** para n= 1, 3, 4, 6, 7, 9, 15, 22, 28, 30, 46,...
  - Existen q^n polinomios en CG(q^n). Ejm: CG(2^3) 0, x, x^2, 1, x+1, x^2+1, x^2+x+1, x^2+x.
  - Hay q^n -1 elementos coprimos con p(x), la identidad de Euler de p(x).
  - Operaciones:
    - **Suma y resta:** c(x)=a(x)+-b(x) mod p(x) consiste en sumar/restar a y b.
    - **Multiplicación**: c(x)=a(x)*b(x) mod p(x)
    - **Dividir(inverso multiplicativo):** u(x)*s(x)=v(x) mod p(x)
      - s(x)^(-1) mod p(x) = s(x)^(Φ(p(x)) -1) mod p(x) = s(x)^(q^n -2) mod p(x)

- **Cuerpos de Galois CG(2^n):** Se representa mediante los coeficientes 0 y 1. El numero de elementos del cuerpo es 2^n. Se emplean n bits para representar un elemento.
  - Ejm: CG(2^3) 0 (0 0 0), x (0 1 0), x^2 (1 0 0), 1 (0 0 1), x+1 (0 1 1), x^2+1 (1 0 1), x^2+x+1 (1 1 1), x^2+x (1 1 0).
  - Operaciones:
    - **Suma y resta**: Consiste en hacer XOR, si son iguales es 0 y si son distintos 1.
      - 101+111=010. 110-011=101. Es sumar sin acarreo.
    - **Multiplicación:** Es la operación lógica AND, es multiplicar los números y sumar con XOR. Si se sobre pasa el grado de p(x), se reduce a mod p(x) o podemos hacerlo dividiendo y cogiendo el resto. 100*100=10000 Habría que dividirlo ya que sobre pasa el grado 3.
    - **División:** Es hallar el inverso multiplicativo, a^(-1)=a^(a^n -2) mod p(x), vamos separando términos y operador hasta reducirlo. Tambien se puede hacer dividiendo normal, buscando que tenga el mismo grado y restando con XOR.
    - **xtime:** Es multiplicar por x, que equivale a multiplicar por 10. Desplazar 1 a la izq. Se utiliza para simplificar, ya que si tiene 0 a la derecha esta multiplicado por 10, y de esta manera podemos reducirlo a multiplicar 10, x veces.
      - Es lo utilizado por los computadores. $100^6=(x^2)^6=x^{12}$. 10 a la 12



- **Restos potenciales:** Son los restos resultado de hacer el modulo n de las potencias de un numero a.
- **Gaussiano:** Es el menor exponente de la base a que da resto 1 modulo n, se busca el mas bajo por lo que si no se encuentra uno por dejo de la identidad de Euler de n, el gaussiano será la identidad de Euler y ademas será generador. Los posible exponentes son divisores de φ(n).
- **Raíces primitivas o generador:** Cuando el gaussiano de un número coincide con la identidad de Euler del modulo. Para calcular si un número lo es, hay que comprobar las potencias con exponentes que sean divisores de la identidad de Euler del modulo, y a la vez que esos valores sean menores que la identidad. Exponentes x: x|φ(n) y x<φ(n)
- **Logaritmos discretos:** Calculó inverso a la exponenciación en la aritmética modular. Para hallar b, buscamos en los restos potenciales de a el valor b, y la columna que contenga el b será la x.
  - a^x=b mod n x=loga(b) mod n