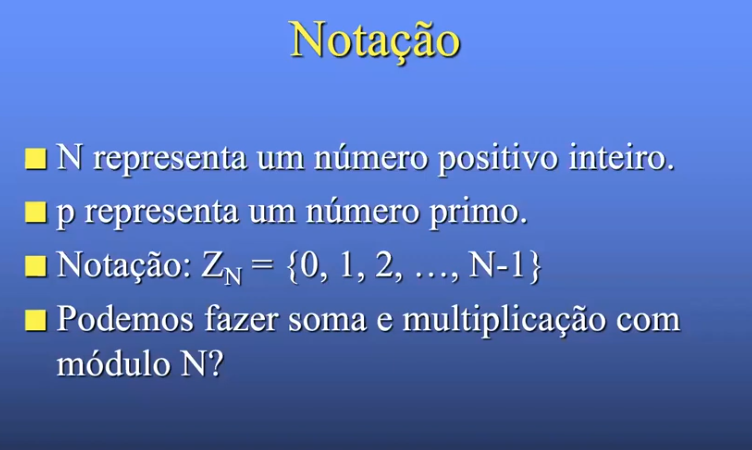
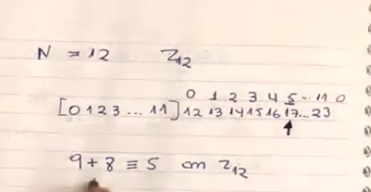
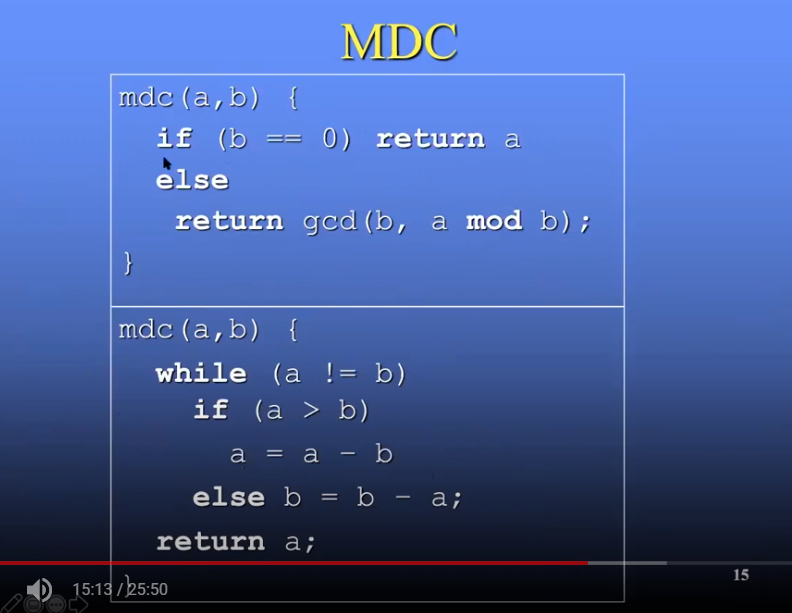
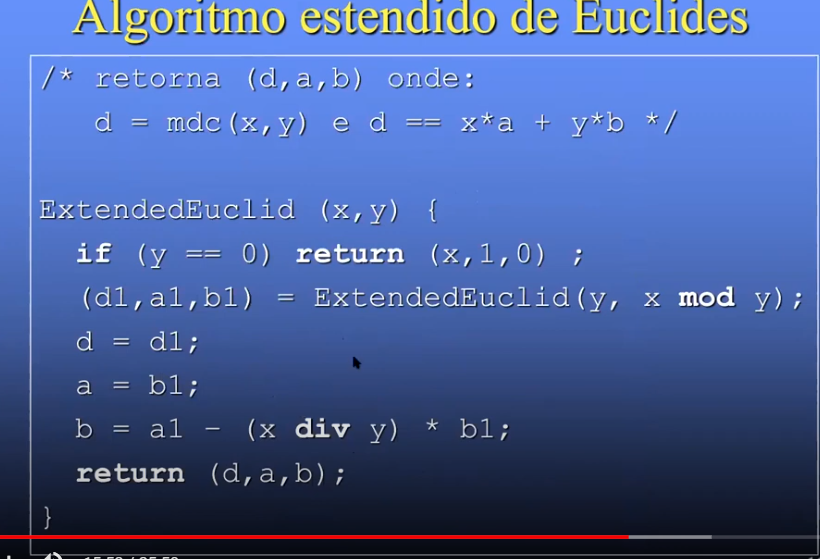
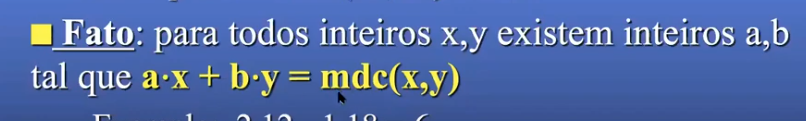
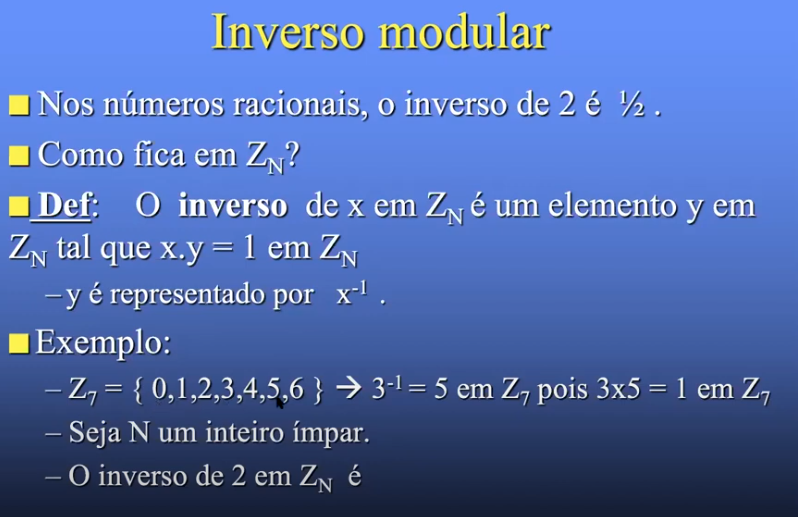
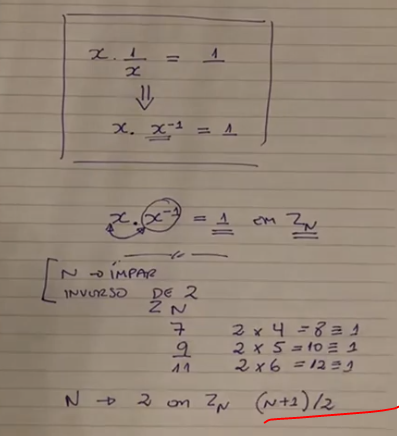
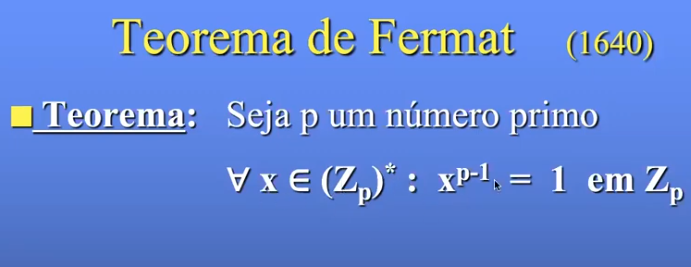
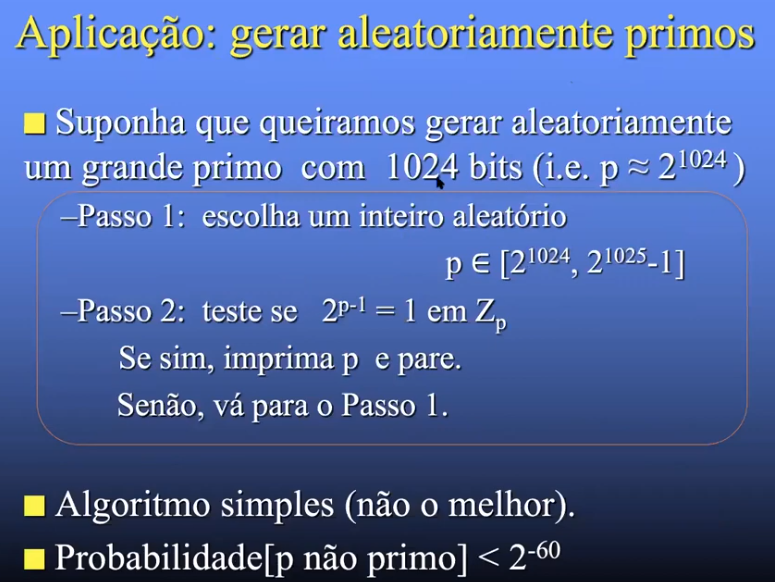
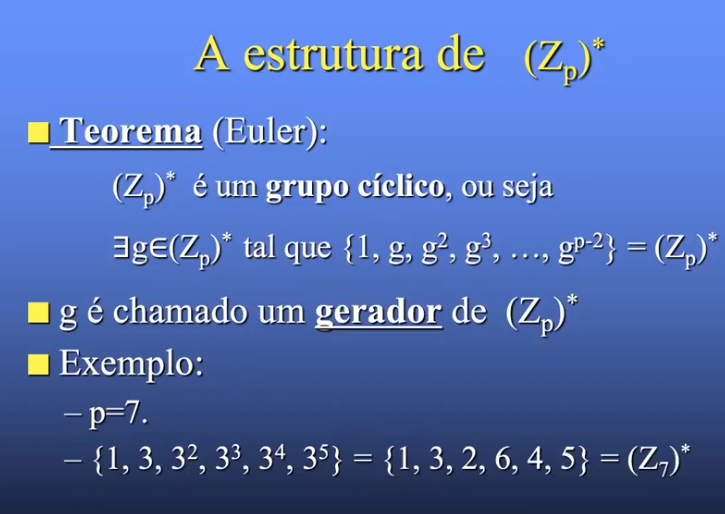
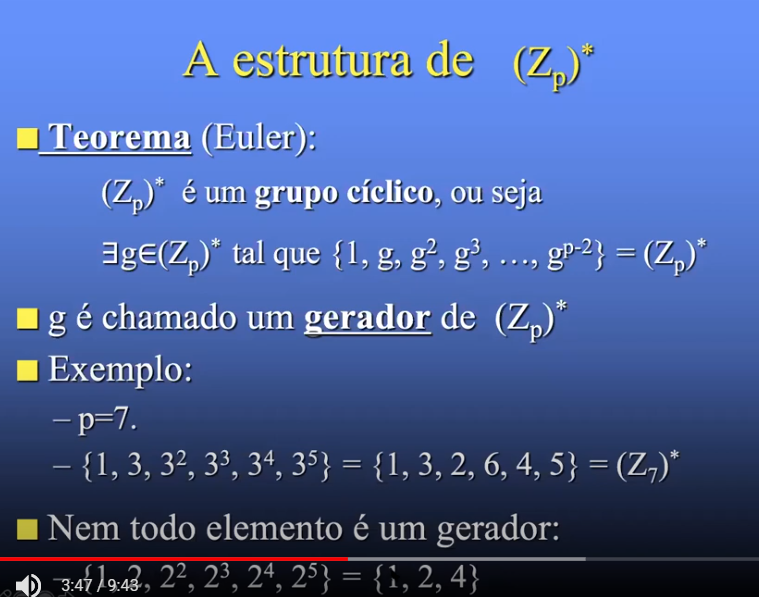
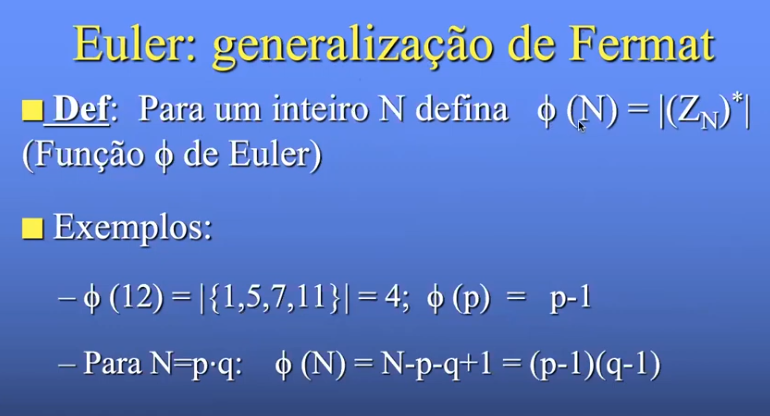
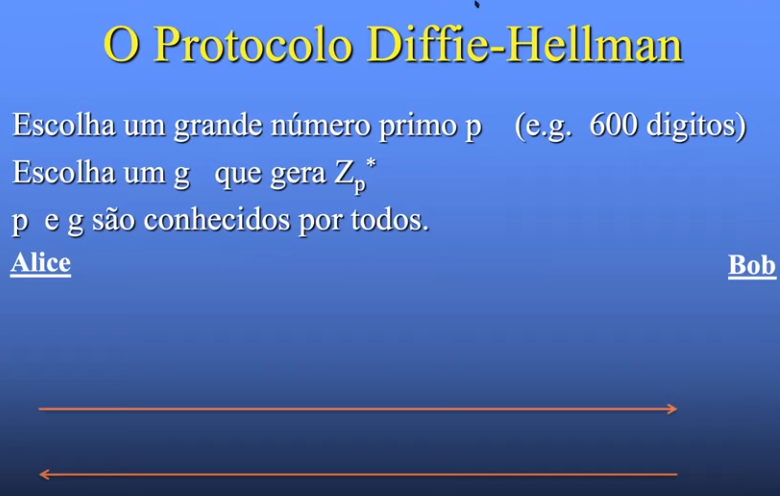
# Aritmética Modular



Exemplo:

* Z de 35 = 0 até 34
* Podemos fazer operações básicas com os módulos, exemplo
  + Z de 12
  + números de 0 a 11
  + 9 + 8 = 5 em Z de 12
    - Significa:
    - 
  + 5 \* 7 = 11 em Z de 12
    - Se pegarmos 35 que é 5\*7 e dividir por 12, o resto da divisão é 11, que é o valor no intervalo de Z de 12 que queremos
  + Pra negativo é feita a soma no módulo, ex:
    - 5 - 7 = 10 em Z de 12
      * 5 - 7 = -2
      * -2 + 12 = 10
* máximo divisor comum:
  + 
  + Dois números são relativamente primos, quando o mdc de dois números é 1;
    - entre si, os dois números são relativamente primos
    - Qualquer número que é menor que p e aior que zero, é relativamente primo em relação a p;
    - Achar o mdc (máximo divisor comum)
      * 
    - Algoritmo estendido de Euclides
      * 
      * Esse retorna o mdc e o a e o b
    - 
      * Acho isso no algoritmo estendido de Euclides
    - Ex.: 9 e 15 não são relativamente primos entre si;
    - inverso: aquele número que multiplico por x e dá 1;
    - Na aritmética modular:
      * 
      * 0 nunca tem inverso
      * O 1 é sempre inverso dele mesmo;
      * O inverso de 6 é o 6 em z de 7
      * Vídeo: <https://www.youtube.com/watch?v=M87tGbj6A74> no minuto 24:58
    - Se tem um n que é ímpar, quem é o inverso de 2?
      * 
  + Teorema de Fermat:
    - 
    - Pra gerar primos aleatórios:
      * 
      * tem uma probabilidade do número gerado não ser primo é muito pequena
  + Teorema de Euler:
    - Gerador é um número dentro de Z de p \*
    - Exemplo, Z de 7, quais os valores que estão em Z de 7? 1, 2, 3, 4, 5, 6
      * Escolho um valor qualquer de Z de 7, no caso vai ser 3 e elevo até p-2 (7-2 = 5);
      * 
      * Nem todo elemento dentro de Z de P é gerador, exemplo o 2:
        + 
      * Euler é uma generalização de Fermat:
        + 
        + a função de euler retorna quantos elementos são relativamente primos a ele;
  + RESUMO:
    - Notação usada:
      * 
      * N é o módulo que estamos trabalhando, e o conjunto vai até N-1
  + Diffie-Hellman
    - 
    - Se escolhe um número grande primo (com uns 600 dígitos);

escolhe um g que gera (conjunto de todos os números que são relativamente primos a p, praticamente todo o conjunto Z de p, pq vai até p-1), significa que qualquer valor que elevar o g

* escolhe um valor a que vai de 1 até p-1;
* pega o g que é conhecido, eleva nesse número aleatório escolhido e faz módulo p, o que vai dar um A grande;
* escolhe outro número aleatório e manda esse B (g elevado na b mod p);
* valor comum de forma que a pessoa no meio do caminho não possa gerar:
  + 
  + os dois ficam com g elevado a ab;