SEGURETAT I PROTECCIÓ DE DADES (GEINF-GDDV, UdG)

CURS 19-20

EXERCICI 2: TEORIA DE NÚMEROS / ARITM. MODULAR

PES: exercici optatiu (pot apujar la nota final fins a un 5%)

DATA LÍMIT ENVIAMENT → dimarts 01/10/19

Aquest exercicis consisteixen en realitzar petits programes en Python segons els requeriments indicats a continuació. Caldrà que els proveu i, en alguns casos, que avalueu el cost en temps per a diferents grandàries de les dades d'entrada

2-a: Feu un programa que donats dos enters (podeu considerar-los majors que 0) calculi el seu MCD usant l'algorisme d'Euclides. Comproveu (taula) com creix el seu cost conforme creix el nombre de dígits dels valors

2-b: A partir del programa anterior, feu-ne un altre que a part de calcular i mostrar el MCD faci el mateix amb les constants de la identitat de Bézoud. Comproveu (taula) com creix el seu cost conforme creix el nombre de dígits dels valors

2-c: Implementeu el test de primalitat que teniu a la diapo 12. Comproveu (taula) com creix el seu cost conforme creix el nombre de dígits del valor

2-d: Implementeu ara un test de primalitat basat al petit teorema de Fermat, indicant si el nombre entrat és primer, no primer de Carmichael, o no primer ni de Carmichael. Feu la mateixa comprovació del cost feta als apartats anteriors.

2-e: Implementeu el programa que descompon un valor positiu en factors primers (diapo 16). Feu la mateixa comprovació del cost feta als apartats anteriors.

2-f: Implementeu un programa que, donat un enter positiu n i un valor enter k, determini si k és inversible a Z/n i, si ho és, calculi el seu invers modular. Feu la mateixa comprovació del cost feta als apartats anteriors.

2-g: Implementeu un programa que calculi la exponenciació modular a Z/n, donat n com a input (a més de la base i l'exponent, és clar). Feu la mateixa comprovació del cost feta als apartats anteriors (aquí podeu augmentar la mida de n, de la base i de l'exponent)

2-h: Feu un programa que calculi el logaritme discret a Z/n, donat n com a input (a més de la base i l'argument, és clar). Feu la mateixa comprovació del cost feta als apartats anteriors (aquí podeu augmentar la mida de n, de la base i de l'argument)

QUÈ CAL LLIURAR AL MOODLE ?

- Codi font dels programes Python
- Document pdf que descrigui les proves realitzades als diferents programes, incloent-hi l'estudi del cost si és requerit

QUÈ ES VALORARÀ ?

- Correctesa de la implementació dels algorismes demanats
- Correctesa del document pdf lliurat

ACLARIMENTS

- Es tracta d'una pràctica individual. *Qualsevol còpia detectada serà penalitzada*.
- Suggerim que useu el llenguatge de programació **Python**, tot i que, si no coneixeu aquest llenguatge i us suposa un inconvenient important aprendre'l, també s'admetran altres llenguatges de programació (C++, Java, ...).