

Haga un programa con el lenguaje de programación Python que presente una calculadora modular con números gigantes de más de 10 o más cifras, la cual puede servir de gran aplicación en criptografía. Deberá presentar mínimamente, por consola:

1. Un menú con suma, multiplicación y división en \mathbb{Z}_n , la potencia modular (exponente y base de la potencia), inversos multiplicativos modulares (si existen), la raíz cuadrada modular de los números ingresado (mostrar, si existen las raíces cuadradas y su cantidad), lista de los cuadrados perfectos (mostrar, si existen, los cuadrados perfectos y su cantidad) en \mathbb{Z}_n . En cada operación deberá darle las opciones para entrar los datos tales como: la base modular, los números correspondientes para el cálculo.
2. El programa debe mostrar: los resultados de cada operación y, en caso de NO EXISTIR, mostrar su adecuado mensaje de error.
3. A pesar de que la recepción de los datos de entrada es por consola, la presentación del menú deberá ser muy buena, precisa y adecuada.

NOTA:

ENTREGUE LA APLICACIÓN EN LA FECHA DEFINIDA

EVITE LA COPIA O FRAUDE; DE NO SERLO ASÍ SE ANULARÁ ESTA Y SE ENVIARÁ COPIA A DECANATURA. RECUERDE: Los grandes corruptos se hacen con pequeños fraudes.

SOLUCIONE ÚNICAMENTE EL PROBLEMA ASIGNADO POR EL PROFESOR

DICHA CALCULADORA MODULAR O EN \mathbb{Z}_n deberá permitir el ingreso de números gigantes (30 o más cifras). En Python no tiene problema.

Datos que debe ingresar el usuario: un número n (entero positivo, obligatorio), un número " a " (no negativo o sea perteneciente a \mathbb{Z}_n) y un número b (entero no negativo o sea perteneciente a \mathbb{Z}_n).

Operaciones que debe calcular:

Suma modular

Producto modular

Inverso modular (número " a " tal que al multiplicarlo modularmente por " a^{-1} " es 1, o sea $a \cdot a^{-1} \equiv 1 \pmod{n}$)

División modular

Potencia modular

Raíz cuadrada modular (mostrar la cantidad de raíces)

Cuadrados perfectos en \mathbb{Z}_n (mostrar la cantidad de cuadrados perfectos)

SUGERENCIA:

$n = \underline{\hspace{2cm}}$	$\mathbb{Z}_n = \{0, 1, 2, 3, \dots, n-1\}$	9	$\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$
$a = \underline{\hspace{2cm}}$	pertenece a \mathbb{Z}_n	21	21 no pertenece a $\mathbb{Z}_9 \Leftrightarrow a \neq 3$
$b = \underline{\hspace{2cm}}$	pertenece a \mathbb{Z}_n	-35	-35 no pertenece a $\mathbb{Z}_9 \Leftrightarrow b \neq 1 \Rightarrow b^{-1} = 1$

Muestre("Entre un número entero positivo")

Lea(n)

Mientras $n \leq 0$

Muestre("Entre un número entero positivo")

Lea(n)

FinMientras

Muestre("Entre un número de \mathbb{Z}_n ")

Lea(a)

```

a=a MOD n    // lo deja en Zn
Muestre("Entre un numero de Zn")
Lea(b)
b=b MOD n    // lo deja en Zn
//Resultados
SumaM=      ProductoM=      PotenciaM=      InvM=
DivisonM=      RaizCuadradaM={ }      CuadradosPerfectosM={ }

```