*****Instituto Politécnico Nacional***

***Escuela Superior de Cómputo***

*Criptography*

***Ejercicios Capítulo VII***

***Nombre:*** *Sampayo Hernández Mauro*

***Grupo:*** *3CV17*

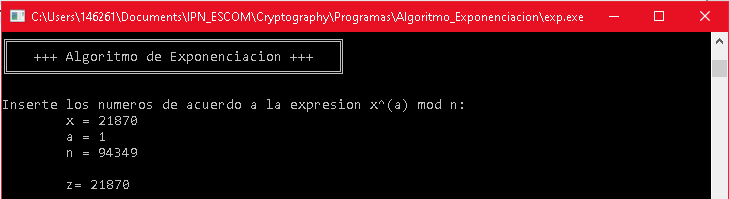
***Profesor:*** *Víctor Manuel Silva García*

**Ejercicios**

1. **Dada la curva , muestre que el punto es solución de la curva. Además, calcule y .**

Primero se inicia con el calculo del valor de

Realizamos el cálculo de :

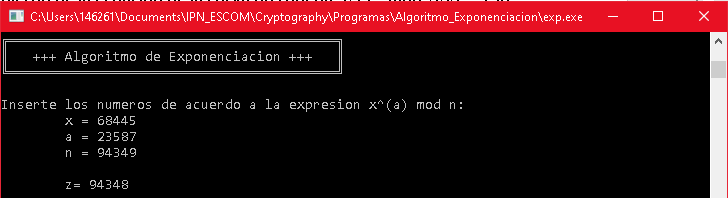


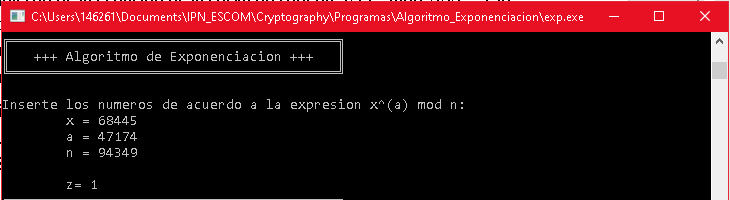
Sacamos el inverso de r mod p, donde y



De esta manera , por lo tanto:

Comprobamos que la constante no sea potencia cuarta de algún elemento del conjunto , pero si potencia cuadrada de algún elemento del campo .

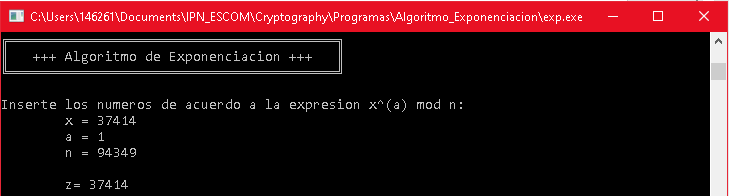




**Con esto podemos comprobar que el punto es solución de la curva**

* **Calculando :**

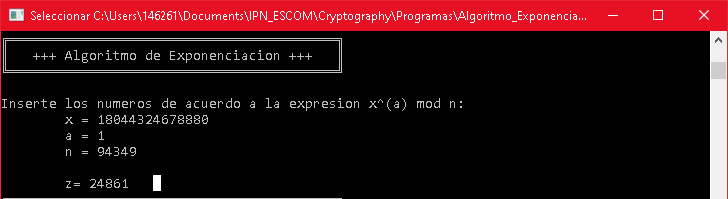
Realizamos el cálculo de :



Sacamos el inverso de r mod p, donde y

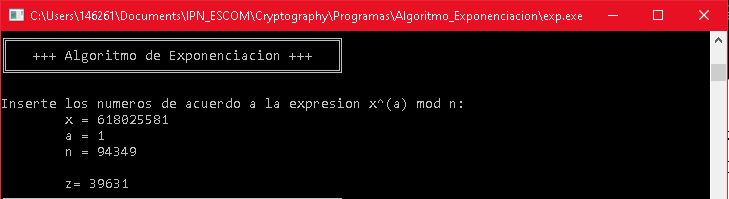


De esta manera , por lo tanto:



mod.

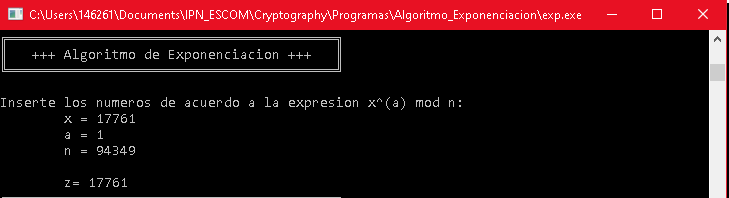
mod 618025581mod



**Así con**

* **Calculando :**

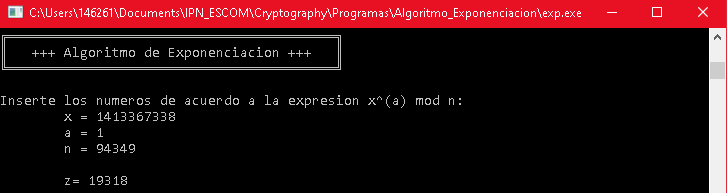
Realizamos el cálculo de :



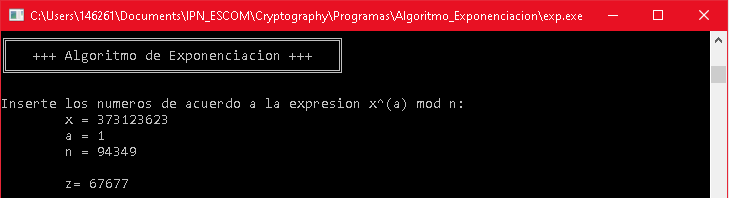
Sacamos el inverso de r mod p, donde y



De esta manera , por lo tanto:

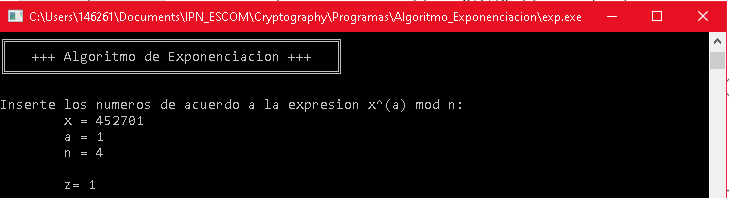


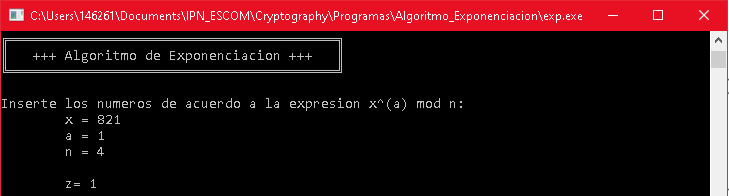
mod 373123623 mod



**Así con**

1. **Dados los valores de y encuentre lo siguiente:**
   1. **El primo y muestre que mod. 4 ≡ 1, además, que +**





* 1. **El orden de la Curva, además, muestre que es primo.**

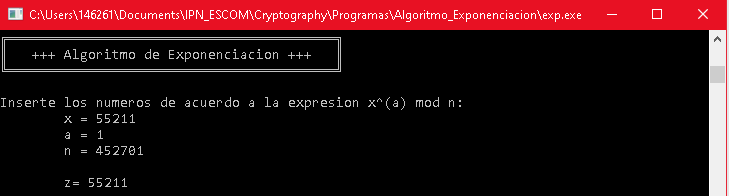


**Por lo tanto, q es un numero Primo**

* 1. **Si α = (55211, 443096) calcule el valor de y muestre que no es potencia cuarta de ningún elemento de ; además, muestre que si es potencia cuadrada de algún elemento de .**

Iniciamos con el cálculo del valor de

Realizamos el cálculo de :

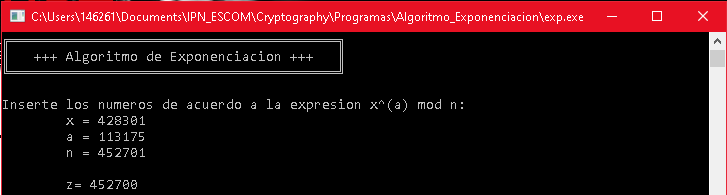


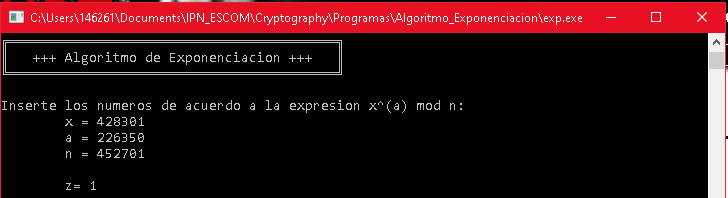
Sacamos el inverso de r mod p, donde y



De esta manera , por lo tanto:

Comprobamos que la constante no sea potencia cuarta de algún elemento del conjunto , pero si potencia cuadrada de algún elemento del campo .

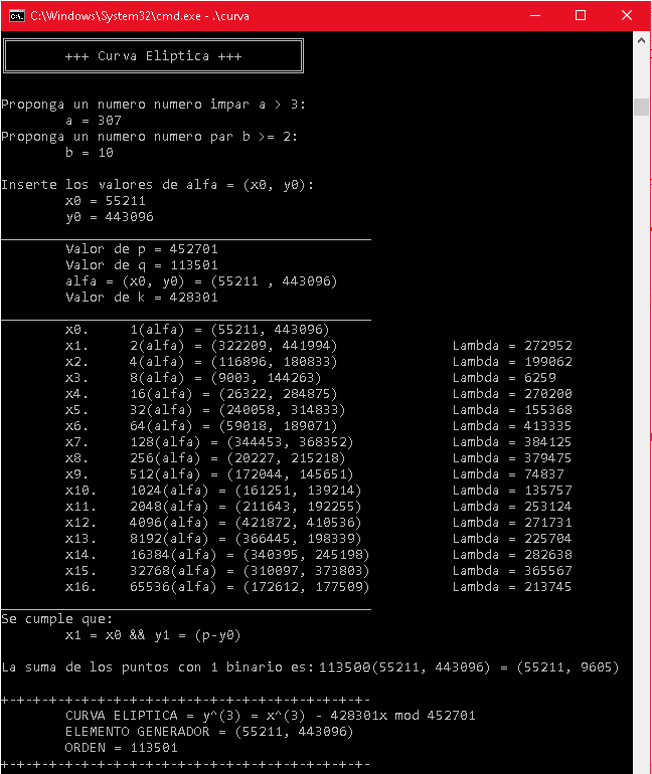




**Por lo tanto , no es potencia cuarta de algún elemento del conjunto , pero si potencia cuadrada de algún elemento del campo .**

1. **Desarrolle el software para encontrar Curvas Elípticas, siguiendo el diagrama de flujo mostrado en la Figura 7.3.1. Muestre que α = (55211, 443096) es un elemento generador para la curva del problema anterior.**

Al final del programa podremos ver el resultado de la comprobación, lo cuál confirma que en efecto, α = (55211, 443096) es un elemento generador

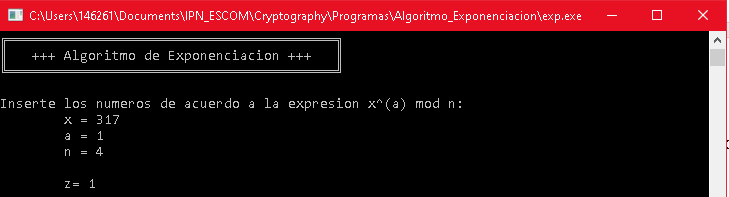


1. **Diga cuál es la expresión de la Curva Elíptica del problema 1. Además, calcule lo solicitado en los siguientes incisos.**

Previo a la resolución del ejercicio, se debe establecer que el primo del problema 1 se construyó de acuerdo con los valores y , pues . Dichos valores se obtuvieron de la siguiente manera:

Proponiendo un valor par para, siendo este se tiene:

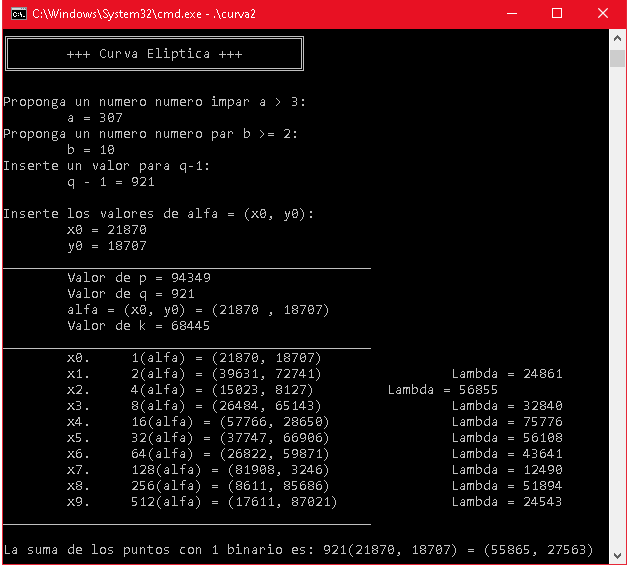
Y dichos valores cumplen con que



La expresión de la curva elíptica del problema 1 es

* 1. **Considerando que 921 es la clave privada realice los cálculos necesarios para encontrar la clave pública .**

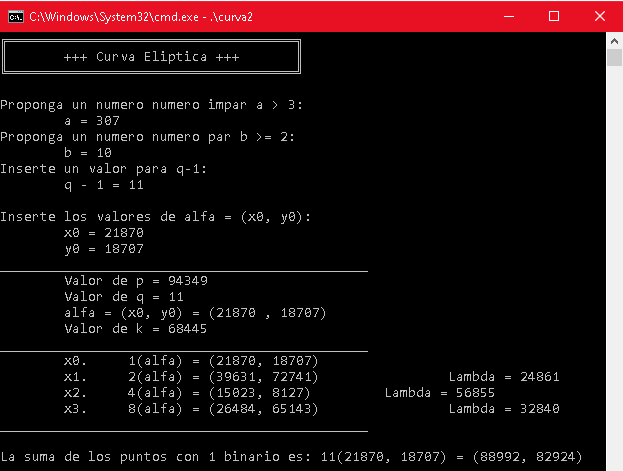
Para facilitar el cálculo de se optó por realizar modificaciones menores a el programa desarrollado en el inciso anterior de tal manera que se adecuasen a los requerimientos del ejercicio**.**



**Por lo tanto**

* 1. **Calcule el punto y cífrelo, esto es, calcule los valores de . También, realice el proceso de descifrado.**

Nuevamente nos auxiliamos del programa modificado para que cálculo de para facilitar su cálculo:



**Por lo tanto**

* **Cifrado del punto :**

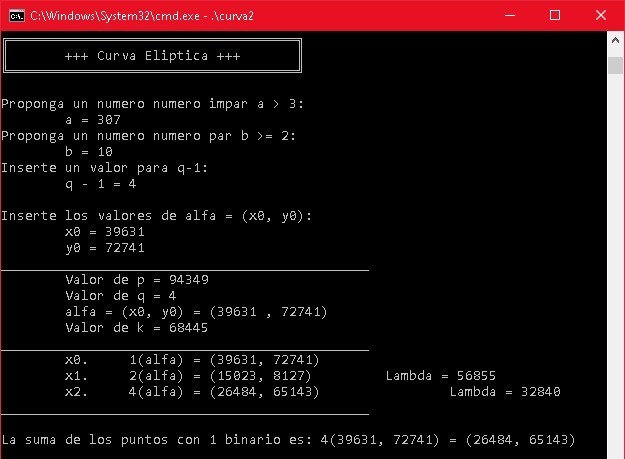
Curva:

Suponiendo que y

**\*\*NOTA:** Este valor ya se obtuvo durante el procedimiento de obtención del valor de y se puede observar en la captura de pantalla del programa, razón por lo que no se mostrará el procedimiento de obtención de este resultado.

**\*\*NOTA:** Este valor ya se calculo anteriormente en el problema 1, por lo que no se mostrará el procedimiento de obtención de este resultado. De igual manera este resultado también se puede observar en la captura de pantalla del programa, durante el procedimiento de obtención del valor de .

Calculando , auxiliándonos del programa modificado, se tiene:



Por lo tanto , así:

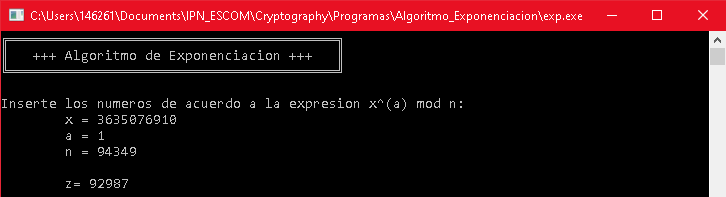
Realizamos el cálculo de :

Sacamos el inverso de r mod p, donde y



De esta manera , por lo tanto:

mod 3635076910 mod

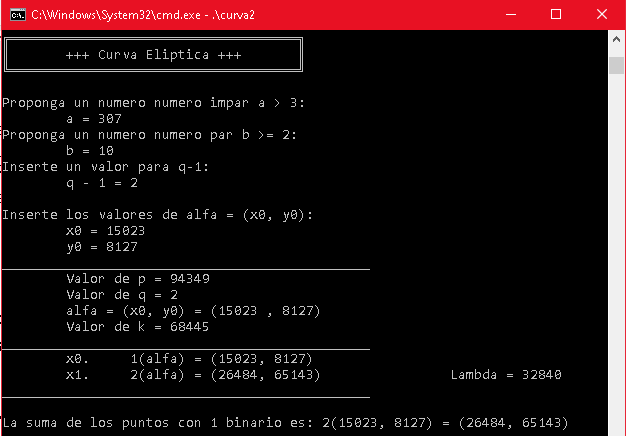


Por lo tanto:

**Así, se tiene que , donde:**

* **Descifrado del punto :**

Calculando , auxiliándonos del programa modificado, se tiene:



Sin embargo como se está buscando el valor de se debe cambiar la segunda coordenada por:

Por lo tanto *,* así:

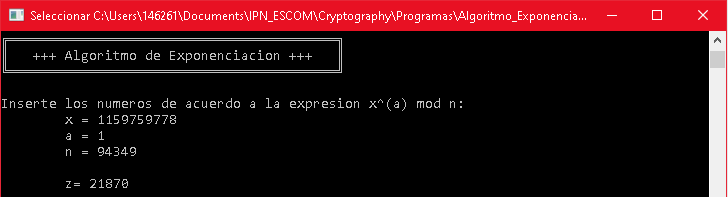
Realizamos el cálculo de :

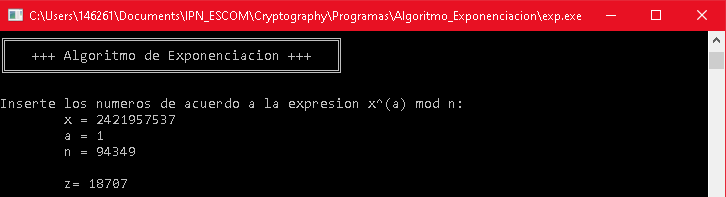
Sacamos el inverso de r mod p, donde y



De esta manera , por lo tanto:

mod 1159759778 mod





**Por lo tanto:**