Tarea 4

1. Pregunta 01

A Factoriza 35 tratando de calcular 3Q.

Para realizar primero sumamos el punto Q 3 veces, para esto usamos un programa en python que nos ayuda a calcular la suma de puntos

```
def suma(self,punto2,a,p):
        x1=self.x
        y1=self.y
        x2=punto2.x
        y2=punto2.y
        if( x1==x2 and ((y1*-1)== y2 )):
            punto3=Punto(-1,-1)
            return punto3
        else:
            punto3=Punto(0,0)
            lambd=punto1.lambd(punto2,a,p)
            punto3.x=((lambd * lambd)-x1-x2)%p
            punto3.y=((lambd*(x1-punto3.x))-y1)%p
        return punto3
```

al pasar los parámetros punto1=(15,-4), 21 y 35, donde (15,-4) es el punto que nos dieron a=21 y p=35, esto nos devuelve (14,22), pero esto unicamente es el punto 2Q, para solucionarlo sumamos 2Q+punto1 y el resultado es (17,21).

Una vez tenemos este punto sacamos la λ=

$$\begin{cases} (3x_1^2 + A) * 2(y_1)^{-1}, & \text{si } P = Q; \\ (y1 - y2) * (x_1 - x_2) & \text{si } P! = Q; \end{cases}$$

En este caso, para sacar la λ estamos nuestra P=(17,21) y Q=(17,21) por lo que tenemos que usar el primer caso, entonces sustituyendo los valores nos queda de la siguiente forma

$(3(17)^2 + 20) * 2(21)^{-1} \rightarrow \frac{867+20}{42^{-1}}$ pero, ya tenemos lo que nos interesa que es el denominador pero recordemos que no estamos trabajando con los números reales por lo cual tenemos que encontrar el inverso de 42 mod 35, pero este número no existe.

Por lo cual tenemos que sacarle el MCD(42,35) que en este caso es 7 $\therefore$ un factor de 35 es 7