Tarea 4

1. Pregunta 01

A Factoriza 35 tratando de calcular 3Q.

Primero para poder realizar esta operación tenemos que enontrar 2Q, para ello tenemos que sumar los puntos (15,4) + (15,4) Recordando que la suma se define de la siguiente forma

P+Q=

$$\begin{cases} Infinito & \text{SI } x_1 = x_2 \;\&\; -y_1 = y_2; \\ (x_3, y_3) & x_3 = (\lambda^2 - x_1 - x_2)\ mod\ p\ y\ y_3 = (\lambda(x_1 - x_3) - x_1)\ mod\ p \end{cases}$$

Pero para esto necesitamos sacar primero a λ que recordemos que se difine de la siguiente manera

λ=

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

Para esto entonces simplemente sustituimos los valores, en lambda debido a que P=Q entonces usamos el primer caso de la lamda lo cual nos dice que $\lambda = (((3(15)^2) + -20) * 2(-4)^{-1}))mod35$
$\rightarrow$ (((3*225)-20* (-8)$^{-1}$)mod 35
$\rightarrow$ ((675-20)*13)mod 35
$\rightarrow$ (655 * 13) mod 35
$\rightarrow$ 8515 mod 35
$\therefore \lambda = 10$

Ahora ya podemos sumar, primero sacaremos x_3 = 10^2-15-15 mod 35
$\rightarrow$ 100-30 mod 35
$\rightarrow$70 mod 35
$\therefore$ x3=0

Ahora debemos sacar a y_3=(10(15-0)- -4) mod 35
$\rightarrow$ 150+4 mod 35
$\rightarrow$ 154 mod 35
$\therefore y_3 = 14$

Entonces ya sabemos el valor del punto 2Q, ahora debemos sumar Q+2q para tener 3Q, para eso debemos calcular de nuevo λ por lo que haremos

λ= $\frac{-4-14}{15-0}$

Aquí encontramos un error debido a que 15 no tiene inverso multiplicativo en el grupo 35 así que eso implica que tenemos que sacar el MCD(35,15) = 5 $\therefore$ 5 es factor de 35.

2 Factoriza 35 tratando de calcular 4Q duplicándolo.

Ahora no calcularemos 2Q debido a que ya lo calculamos anteriormente en el ejercicio 1 por lo cual pasaremos a calcular λ bajo la definición del ejercicio 1

$\lambda = \frac{3(0)^2}{2(14)}$mod 35

Encontramos de nuevo el mismo problema que en el ejercicio anterior debido a que 28 mod 35 no tiene inverso, por lo cual debemos sacar su MCD(28,35) = 7 $\therefore$ 7 es un factor de 35

3 Calcula 3Q y 4Q sobre E (mod 5) y sobre E (mod 7) explica por que el factor 5 se obtiene calculando 3Q y por que el factor 7 se obtiene calculando 4Q.

Debido a que cuando calculas 3Q , intentamos sacar el inverso de 15 en el grupo 35, esto conflictuá ya que como 15 y 35 no son primos $\rightarrow$ que son números compuesto por primos esto nos lo sabemos por el teorema fundamental de la aritmética , ahora al sacar su MCD descubrimos que 5 es ese número $\therefore$ por esa razón 3 q , nos dio el valor 5 por compartir ese primo con 15 y análogamente pasa lo mismo con 28 y 35

Ahora el valor de 3 Q con 5 = No se puede calcular debido a que tenemos que cuando intentamos sumar Q= (15,-4) con 2Q=(0,4)(Los calculos de como se llego a 2q se dejan como ejercicio para el lector) e intentamos sacar α = (-4-4).(0-15)$^{-1}$
$\rightarrow$ 8 . (-15)$^{-1}$ y como -15 no esta en el campo de 5 entonces lo que hacemos es devolverlo con la operación modulo $\rightarrow$ -15 mod 5 = 0 y 0 no tiene inverso multiplicativo en 5 por lo que nuestro proceso termina aquí.

Ahora sacaremos el punto 4 Q sumando 2Q + 2Q lo sacamos la λ=3, haciendo los cálculos llegamos a que $x_3 = 0 \wedge y_3 = 4 \therefore$ Q3 = (0,4)

Nos falta sacar los valores de 3Q y 4Q en el modulo 7 por lo que tenemos que calcular 2Q al igual que tratamos al modulo 5 los calculos se dejaran al lector, entonces llegamos a 2Q=(0,0) por lo que ahora pasamos a sumar Q=(15,-4) + 2Q=(0,0) llegamos a que $\lambda = 4$ por lo que x_3=1 y $y_3 = 5$, $\therefore$ Q_3 = (1,5)

Para finalizar solo nos falta calcular a 4Q por lo que tenemos que sumar 2Q + 2Q, pero esta no se puede debido a que cuando queremos calcular la λ llegamos a los siguiente = $(3(0)^2$-20 * $(2 * 0)^{-1}$) y ya que no podemos sacar el inverso de 0 mod 7 debido a que no existe