MOOC de Criptología Matemática. Operaciones con Puntos

Leandro Marín

Módulo III. Sesión 3.
Dificultad Alta

Casos Especiales

- Ya hemos visto que los puntos racionales de una curva elíptica tienen estructura de grupo, por lo que se pueden sumar.

Casos Especiales

- Ya hemos visto que los puntos racionales de una curva elíptica tienen estructura de grupo, por lo que se pueden sumar.
- Si estamos en un cuerpo $K = \mathbb{Z}_p$ y una curva $y^2 = x^3 + ax + b$, lo primero que podemos ver es que el punto del infinito de esta curva es $(0 : 1 : 0)$ que usaremos como elemento O, el elemento neutro del grupo.

Casos Especiales

- Ya hemos visto que los puntos racionales de una curva elíptica tienen estructura de grupo, por lo que se pueden sumar.
- Si estamos en un cuerpo $K = \mathbb{Z}_p$ y una curva $y^2 = x^3 + ax + b$, lo primero que podemos ver es que el punto del infinito de esta curva es $(0 : 1 : 0)$ que usaremos como elemento O, el elemento neutro del grupo.
- Dado cualquier punto P, sabemos por definición que $P + O = P = O + P$.

Casos Especiales

- Ya hemos visto que los puntos racionales de una curva elíptica tienen estructura de grupo, por lo que se pueden sumar.
- Si estamos en un cuerpo $K = \mathbb{Z}_p$ y una curva $y^2 = x^3 + ax + b$, lo primero que podemos ver es que el punto del infinito de esta curva es $(0 : 1 : 0)$ que usaremos como elemento O, el elemento neutro del grupo.
- Dado cualquier punto P, sabemos por definición que $P + O = P = O + P$.
- También podemos ver que si $P = (x, y)$ está en la curva, el punto $(x, -y)$ también está.

Casos Especiales

- Ya hemos visto que los puntos racionales de una curva elíptica tienen estructura de grupo, por lo que se pueden sumar.
- Si estamos en un cuerpo $K = \mathbb{Z}_p$ y una curva $y^2 = x^3 + ax + b$, lo primero que podemos ver es que el punto del infinito de esta curva es $(0 : 1 : 0)$ que usaremos como elemento O, el elemento neutro del grupo.
- Dado cualquier punto P, sabemos por definición que $P + O = P = O + P$.
- También podemos ver que si $P = (x, y)$ está en la curva, el punto $(x, -y)$ también está.
- Estos puntos serán opuestos en la estructura de grupo, es decir $(x, y) + (x, -y) = O$ para cualquier punto $P = (x, y)$ de la curva, por lo tanto $-P = (x, -y)$ tal y como sucedía en nuestro ejemplo.

Suma de Puntos Distintos

- Supongamos ahora que $P_1 = (x_1, y_1)$ y $P_2 = (x_2, y_2)$ son puntos afines de la curva que no son opuestos, es decir, $(x_2, y_2) \neq (x_1, -y_1)$.

Suma de Puntos Distintos

- Supongamos ahora que $P_1 = (x_1, y_1)$ y $P_2 = (x_2, y_2)$ son puntos afines de la curva que no son opuestos, es decir, $(x_2, y_2) \neq (x_1, -y_1)$.
- Si P_1 y P_2 son puntos distintos de la curva, podemos trazar la recta que une estos dos puntos. Dicha recta cortará a la curva en un tercer punto por tratarse de una curva de tercer grado. Si llamamos R a esta intersección, la relación que define la estructura de grupo es que $P_1 + P_2 + R = 0$ y por lo tanto $P_1 + P_2 = -R$.

Suma de Puntos Distintos

- Supongamos ahora que $P_1 = (x_1, y_1)$ y $P_2 = (x_2, y_2)$ son puntos afines de la curva que no son opuestos, es decir, $(x_2, y_2) \neq (x_1, -y_1)$.
- Si P_1 y P_2 son puntos distintos de la curva, podemos trazar la recta que une estos dos puntos. Dicha recta cortará a la curva en un tercer punto por tratarse de una curva de tercer grado. Si llamamos R a esta intersección, la relación que define la estructura de grupo es que $P_1 + P_2 + R = 0$ y por lo tanto $P_1 + P_2 = -R$.
- Encontrar el punto $-R$ de este modo requeriría resolver una serie de ecuaciones, aunque podemos simplemente tomar la pendiente de la recta $m = \frac{y_1 - y_2}{x_1 - x_2}$ y luego poner

$$x_3 = -x_1 - x_2 + m^2 \quad y_3 = -y_1 + m(x_1 - x_3)$$

Suma de Puntos Distintos

- Supongamos ahora que $P_1 = (x_1, y_1)$ y $P_2 = (x_2, y_2)$ son puntos afines de la curva que no son opuestos, es decir, $(x_2, y_2) \neq (x_1, -y_1)$.
- Si P_1 y P_2 son puntos distintos de la curva, podemos trazar la recta que une estos dos puntos. Dicha recta cortará a la curva en un tercer punto por tratarse de una curva de tercer grado. Si llamamos R a esta intersección, la relación que define la estructura de grupo es que $P_1 + P_2 + R = 0$ y por lo tanto $P_1 + P_2 = -R$.
- Encontrar el punto $-R$ de este modo requeriría resolver una serie de ecuaciones, aunque podemos simplemente tomar la pendiente de la recta $m = \frac{y_1 - y_2}{x_1 - x_2}$ y luego poner

$$x_3 = -x_1 - x_2 + m^2 \quad y_3 = -y_1 + m(x_1 - x_3)$$

- El punto $P_1 + P_2$ es precisamente (x_3, y_3).

Suma de Puntos Iguales

- También se nos puede dar el caso de tener que sumar un punto $P = (x_1, y_1)$ consigo mismo, es decir $P + P = 2P$.

Suma de Puntos Iguales

- También se nos puede dar el caso de tener que sumar un punto $P = (x_1, y_1)$ consigo mismo, es decir $P + P = 2P$.
- En este caso, en lugar de tomar la recta que une P con P, debemos tomar la recta tangente a la curva en el punto P, que cortará a la curva en un punto R del que obtendremos la fórmula $2P + R = 0$ y por lo tanto $2P = -R$.

Suma de Puntos Iguales

- También se nos puede dar el caso de tener que sumar un punto $P = (x_1, y_1)$ consigo mismo, es decir $P + P = 2P$.
- En este caso, en lugar de tomar la recta que une P con P, debemos tomar la recta tangente a la curva en el punto P, que cortará a la curva en un punto R del que obtendremos la fórmula $2P + R = 0$ y por lo tanto $2P = -R$.
- Aplicando las fórmulas, en este caso la pendiente de la recta tangente es $m = \frac{3x_1^2+a}{2y_1}$.

Suma de Puntos Iguales

- También se nos puede dar el caso de tener que sumar un punto $P = (x_1, y_1)$ consigo mismo, es decir $P + P = 2P$.
- En este caso, en lugar de tomar la recta que une P con P, debemos tomar la recta tangente a la curva en el punto P, que cortará a la curva en un punto R del que obtendremos la fórmula $2P + R = 0$ y por lo tanto $2P = -R$.
- Aplicando las fórmulas, en este caso la pendiente de la recta tangente es $m = \frac{3x_1^2+a}{2y_1}$.
- El resto de las ecuaciones son iguales $2P = (x_3, y_3)$ con

$$x_3 = -x_1 - x_1 + m^2 \quad y_3 = -y_1 + m(x_1 - x_3)$$

Suma de Puntos Iguales

- También se nos puede dar el caso de tener que sumar un punto $P = (x_1, y_1)$ consigo mismo, es decir $P + P = 2P$.
- En este caso, en lugar de tomar la recta que une P con P, debemos tomar la recta tangente a la curva en el punto P, que cortará a la curva en un punto R del que obtendremos la fórmula $2P + R = 0$ y por lo tanto $2P = -R$.
- Aplicando las fórmulas, en este caso la pendiente de la recta tangente es $m = \frac{3x_1^2 + a}{2y_1}$.
- El resto de las ecuaciones son iguales $2P = (x_3, y_3)$ con

$$x_3 = -x_1 - x_1 + m^2 \quad y_3 = -y_1 + m(x_1 - x_3)$$

- Como se puede apreciar necesitamos que la curva tenga tangentes en todo punto, por eso es necesaria la no singularidad de la curva en la definición.

Definición

- Sea k un número natural, y P un punto en una curva elíptica.

Definición

- Sea k un número natural, y P un punto en una curva elíptica.
- Definiremos $kP = \underbrace{P + P + \cdots + P}_{k \;\; veces}$, entendiendo que $0P = O$.

Definición

- Sea k un número natural, y P un punto en una curva elíptica.
- Definiremos $kP = \underbrace{P + P + \cdots + P}_{k \ \ veces}$, entendiendo que $0P = O$.
- De esta forma tendremos $1P = P$, $2P = P + P$, etc.

Definición

- Sea k un número natural, y P un punto en una curva elíptica.
- Definiremos $kP = \underbrace{P + P + \cdots + P}_{k \ \ veces}$, entendiendo que $0P = O$.
- De esta forma tendremos $1P = P$, $2P = P + P$, etc.
- Para valores negativos, podremos $-kP = k(-P)$ siendo $-P$ el opuesto de P en la estructura de grupo.

Definición

- Sea k un número natural, y P un punto en una curva elíptica.
- Definiremos $kP = \underbrace{P + P + \cdots + P}_{k \ \ veces}$, entendiendo que $0P = O$.
- De esta forma tendremos $1P = P$, $2P = P + P$, etc.
- Para valores negativos, podremos $-kP = k(-P)$ siendo $-P$ el opuesto de P en la estructura de grupo.
- De esta forma podemos multiplicar cualquier número entero por puntos de la curva.

Propiedades de la Multiplicación Escalar

- Dados $k, t \in \mathbb{Z}$ y P, Q puntos cualesquiera de la curva, se cumple que

Propiedades de la Multiplicación Escalar

- Dados $k, t \in \mathbb{Z}$ y P, Q puntos cualesquiera de la curva, se cumple que
  - $(k + t)P = kP + tP$

Propiedades de la Multiplicación Escalar

- Dados $k, t \in \mathbb{Z}$ y P, Q puntos cualesquiera de la curva, se cumple que
  - $(k + t)P = kP + tP$
  - $(kt)P = k(tP)$

Propiedades de la Multiplicación Escalar

- Dados $k, t \in \mathbb{Z}$ y P, Q puntos cualesquiera de la curva, se cumple que
  - $(k + t)P = kP + tP$
  - $(kt)P = k(tP)$
  - $k(P + Q) = kP + kQ$
- Si n es el número de puntos racionales de la curva elíptica se cumple que $nP = O$ para cualquier punto P de la curva.

Cálculo de la Multiplicación Escalar I

- Para las aplicaciones criptográficas es necesario el cálculo de valores kP para números k que pueden tener más de 100 cifras.

Cálculo de la Multiplicación Escalar I

- Para las aplicaciones criptográficas es necesario el cálculo de valores kP para números k que pueden tener más de 100 cifras.
- Por lo tanto es totalmente inviable hacer el cálculo como $\underbrace{P + P + \cdots + P}_{k \ \ veces}$.

Cálculo de la Multiplicación Escalar I

- Para las aplicaciones criptográficas es necesario el cálculo de valores kP para números k que pueden tener más de 100 cifras.
- Por lo tanto es totalmente inviable hacer el cálculo como $\underbrace{P + P + \cdots + P}_{k \ \ veces}$.
- Es lo mismo que nos sucedía en el caso del RSA para calcular $x^d (mod \ \ n)$

Cálculo de la Multiplicación Escalar I

- Para las aplicaciones criptográficas es necesario el cálculo de valores kP para números k que pueden tener más de 100 cifras.
- Por lo tanto es totalmente inviable hacer el cálculo como $\underbrace{P + P + \cdots + P}_{k \ \ veces}$.
- Es lo mismo que nos sucedía en el caso del RSA para calcular $x^d(mod \ n)$
- Podemos reducir el cálculo de kP al cálculo de un número reducido de sumas de puntos con la ayuda de un acumulador.

Cálculo de la Multiplicación Escalar II

- ENTRADA: $k = \sum_{i=0}^{t-1} k_i 2^i,\ P$

Cálculo de la Multiplicación Escalar II

- ENTRADA: $k = \sum_{i=0}^{t-1} k_i 2^i$, P
- SALIDA: kP

Cálculo de la Multiplicación Escalar II

- ENTRADA: $k = \sum_{i=0}^{t-1} k_i 2^i$, P
- SALIDA: kP
- $A \leftarrow O$

Cálculo de la Multiplicación Escalar II

- ENTRADA: $k = \sum_{i=0}^{t-1} k_i 2^i$, P
- SALIDA: kP
- $A \leftarrow O$
- Para i desde $t-1$ hasta 0.

Cálculo de la Multiplicación Escalar II

- ENTRADA: $k = \sum_{i=0}^{t-1} k_i 2^i$, P
- SALIDA: kP
- $A \leftarrow O$
- Para i desde $t-1$ hasta 0.
  - $A \leftarrow 2A$.

Cálculo de la Multiplicación Escalar II

- ENTRADA: $k = \sum_{i=0}^{t-1} k_i 2^i$, P
- SALIDA: kP
- $A \leftarrow O$
- Para i desde $t-1$ hasta 0.
  - $A \leftarrow 2A$.
  - Si $k_i = 1$ entonces $A \leftarrow A + P$.

Cálculo de la Multiplicación Escalar II

- ENTRADA: $k = \sum_{i=0}^{t-1} k_i 2^i$, P
- SALIDA: kP
- $A \leftarrow O$
- Para i desde $t-1$ hasta 0.
  - $A \leftarrow 2A$.
  - Si $k_i = 1$ entonces $A \leftarrow A + P$.
- Devolver A

Ejemplo I

- Consideremos la curva $y^2 = x^3 + 2x + 1$ y el punto $P = (0, 4)$.

Ejemplo I

- Consideremos la curva $y^2 = x^3 + 2x + 1$ y el punto $P = (0, 4)$.
- Usaremos la tabla de suma del grupo que ya vimos para este ejemplo anteriormente:

$+$	$(0,1)$	$(0,4)$	$(1,2)$	$(1,3)$	$(3,2)$	$(3,3)$
$(0,1)$	$(1,3)$	O	$(0,4)$	$(3,3)$	$(1,2)$	$(3,2)$
$(0,4)$	O	$(1,2)$	$(3,2)$	$(0,1)$	$(3,3)$	$(1,3)$
$(1,2)$	$(0,4)$	$(3,2)$	$(3,3)$	O	$(1,3)$	$(0,1)$
$(1,3)$	$(3,3)$	$(0,1)$	O	$(3,2)$	$(0,4)$	$(1,2)$
$(3,2)$	$(1,2)$	$(3,3)$	$(1,3)$	$(0,4)$	$(0,1)$	O
$(3,3)$	$(3,2)$	$(1,3)$	$(0,1)$	$(1,2)$	O	$(0,4)$

Ejemplo I

- Consideremos la curva $y^2 = x^3 + 2x + 1$ y el punto $P = (0, 4)$.
- Usaremos la tabla de suma del grupo que ya vimos para este ejemplo anteriormente:

$+$	$(0,1)$	$(0,4)$	$(1,2)$	$(1,3)$	$(3,2)$	$(3,3)$
$(0,1)$	$(1,3)$	O	$(0,4)$	$(3,3)$	$(1,2)$	$(3,2)$
$(0,4)$	O	$(1,2)$	$(3,2)$	$(0,1)$	$(3,3)$	$(1,3)$
$(1,2)$	$(0,4)$	$(3,2)$	$(3,3)$	O	$(1,3)$	$(0,1)$
$(1,3)$	$(3,3)$	$(0,1)$	O	$(3,2)$	$(0,4)$	$(1,2)$
$(3,2)$	$(1,2)$	$(3,3)$	$(1,3)$	$(0,4)$	$(0,1)$	O
$(3,3)$	$(3,2)$	$(1,3)$	$(0,1)$	$(1,2)$	O	$(0,4)$

- Calcularemos $6P$, por tanto $k = 6$ que escrito en binario es $k = 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$ con lo que $k_2 = 1$, $k_1 = 1$, $k_0 = 0$.

Ejemplo II

- Inicializamos $A \leftarrow O$.

Ejemplo II

- Inicializamos $A \leftarrow O$.
- Para $i = 2$ calculamos $A \leftarrow A + A = O + O = O \; (= 0P)$

Ejemplo II

- Inicializamos $A \leftarrow O$.
- Para $i = 2$ calculamos $A \leftarrow A + A = O + O = O$ $(= 0P)$
- Como $k_2 = 1$ calculamos $A \leftarrow A + P = O + (0, 4) = (0, 4)$ $(= 1P)$

Ejemplo II

- Inicializamos $A \leftarrow O$.
- Para $i = 2$ calculamos $A \leftarrow A + A = O + O = O$ $(= 0P)$
- Como $k_2 = 1$ calculamos $A \leftarrow A + P = O + (0, 4) = (0, 4)$ $(= 1P)$
- Para $i = 1$ calculamos $A \leftarrow A + A = (0, 4) + (0, 4) = (1, 2)$ $(= 2P)$

Ejemplo II

- Inicializamos $A \leftarrow O$.
- Para $i = 2$ calculamos $A \leftarrow A + A = O + O = O$ $(= 0P)$
- Como $k_2 = 1$ calculamos $A \leftarrow A + P = O + (0, 4) = (0, 4)$ $(= 1P)$
- Para $i = 1$ calculamos $A \leftarrow A + A = (0, 4) + (0, 4) = (1, 2)$ $(= 2P)$
- Como $k_1 = 1$ calculamos $A \leftarrow A + P = (1, 2) + (0, 4) = (3, 2)$ $(= 3P)$

Ejemplo II

- Inicializamos $A \leftarrow O$.
- Para $i = 2$ calculamos $A \leftarrow A + A = O + O = O$ $(= 0P)$
- Como $k_2 = 1$ calculamos $A \leftarrow A + P = O + (0, 4) = (0, 4)$ $(= 1P)$
- Para $i = 1$ calculamos $A \leftarrow A + A = (0, 4) + (0, 4) = (1, 2)$ $(= 2P)$
- Como $k_1 = 1$ calculamos $A \leftarrow A + P = (1, 2) + (0, 4) = (3, 2)$ $(= 3P)$
- Para $i = 0$ calculamos $A \leftarrow A + A = (3, 2) + (3, 2) = (0, 1)$ $(= 6P)$

Ejemplo II

- Inicializamos $A \leftarrow O$.
- Para $i = 2$ calculamos $A \leftarrow A + A = O + O = O$ $(= 0P)$
- Como $k_2 = 1$ calculamos $A \leftarrow A + P = O + (0,4) = (0,4)$ $(= 1P)$
- Para $i = 1$ calculamos $A \leftarrow A + A = (0,4) + (0,4) = (1,2)$ $(= 2P)$
- Como $k_1 = 1$ calculamos $A \leftarrow A + P = (1,2) + (0,4) = (3,2)$ $(= 3P)$
- Para $i = 0$ calculamos $A \leftarrow A + A = (3,2) + (3,2) = (0,1)$ $(= 6P)$
- Devolvemos $(0,1) = 6P$

Ejemplo II

- Inicializamos $A \leftarrow O$.
- Para $i = 2$ calculamos $A \leftarrow A + A = O + O = O$ $(= 0P)$
- Como $k_2 = 1$ calculamos $A \leftarrow A + P = O + (0, 4) = (0, 4)$ $(= 1P)$
- Para $i = 1$ calculamos $A \leftarrow A + A = (0, 4) + (0, 4) = (1, 2)$ $(= 2P)$
- Como $k_1 = 1$ calculamos $A \leftarrow A + P = (1, 2) + (0, 4) = (3, 2)$ $(= 3P)$
- Para $i = 0$ calculamos $A \leftarrow A + A = (3, 2) + (3, 2) = (0, 1)$ $(= 6P)$
- Devolvemos $(0, 1) = 6P$

- Como podemos ver $(0, 1) = 6P$ es igual a $-P = -(0, 4) = (0, -4)$ ya que $6P + P = 7P = O$ puesto que el número de puntos de la curva es 7.

Complejidad del Algoritmo

- Como podemos ver, el número de veces que se realiza la operación $A+A$ es igual al número de cifras de k, es decir $log_2(k)$.

Complejidad del Algoritmo

- Como podemos ver, el número de veces que se realiza la operación $A + A$ es igual al número de cifras de k, es decir $log_2(k)$.
- Suponiendo que el número de ceros y unos entre las cifras de k es similar, el número de veces que realizaremos la operación $A + P$ es $\frac{1}{2} log_2(k)$

Complejidad del Algoritmo

- Como podemos ver, el número de veces que se realiza la operación $A + A$ es igual al número de cifras de k, es decir $log_2(k)$.
- Suponiendo que el número de ceros y unos entre las cifras de k es similar, el número de veces que realizaremos la operación $A + P$ es $\frac{1}{2}log_2(k)$
- Por tanto este algoritmo hará un número de operaciones de punto del orden de $\frac{3}{2}log_2(k)$.