# MOOC de Criptología Matemática. Cuestiones de Implementación

Leandro Marín

Módulo III. Sesión 5.
Dificultad Muy Alta

# Introducción

- La operación fundamental en criptografía de curvas elípticas es la multiplicación escalar.

# Introducción

- La operación fundamental en criptografía de curvas elípticas es la multiplicación escalar.
- Esa operación $kP$ ya hemos visto que se puede reducir a una serie de operaciones de punto, tanto de suma de puntos iguales o diferentes.

# Introducción

- La operación fundamental en criptografía de curvas elípticas es la multiplicación escalar.
- Esa operación $kP$ ya hemos visto que se puede reducir a una serie de operaciones de punto, tanto de suma de puntos iguales o diferentes.
- Las operaciones de suma de puntos se reducen a sumas, restas, multiplicaciones y cálculo de inversos.

# Introducción

- La operación fundamental en criptografía de curvas elípticas es la multiplicación escalar.
- Esa operación $kP$ ya hemos visto que se puede reducir a una serie de operaciones de punto, tanto de suma de puntos iguales o diferentes.
- Las operaciones de suma de puntos se reducen a sumas, restas, multiplicaciones y cálculo de inversos.
- Lo que vamos a estudiar en este tema es la forma de hacerlo con el menor coste posible.

# Coste de las Operaciones Básicas

- Las operaciones básicas son la suma, resta, multiplicación y cálculo de inversos en el cuerpo $\mathbb{Z}_p$ para un número primo $p$ de entre 160 y 256 cifras binarias.

# Coste de las Operaciones Básicas

- Las operaciones básicas son la suma, resta, multiplicación y cálculo de inversos en el cuerpo $\mathbb{Z}_p$ para un número primo $p$ de entre 160 y 256 cifras binarias.
- Las operaciones de suma y resta tienen una complejidad del orden de la longitud de los parámetros. El coste es realmente despreciable en comparación con el resto de las operaciones.

# Coste de las Operaciones Básicas

- Las operaciones básicas son la suma, resta, multiplicación y cálculo de inversos en el cuerpo $\mathbb{Z}_p$ para un número primo $p$ de entre 160 y 256 cifras binarias.
- Las operaciones de suma y resta tienen una complejidad del orden de la longitud de los parámetros. El coste es realmente despreciable en comparación con el resto de las operaciones.
- Para poder hacer una operación de multiplicación con el algoritmo de lápiz y papel necesitamos realizar un número de sumas que depende de la longitud de los parámetros. Este algoritmo tiene una complejidad cuadrática.

# Coste de las Operaciones Básicas

- Las operaciones básicas son la suma, resta, multiplicación y cálculo de inversos en el cuerpo $\mathbb{Z}_p$ para un número primo $p$ de entre 160 y 256 cifras binarias.
- Las operaciones de suma y resta tienen una complejidad del orden de la longitud de los parámetros. El coste es realmente despreciable en comparación con el resto de las operaciones.
- Para poder hacer una operación de multiplicación con el algoritmo de lápiz y papel necesitamos realizar un número de sumas que depende de la longitud de los parámetros. Este algoritmo tiene una complejidad cuadrática.
- El cálculo de inversos modulares mediante el algoritmo de Euclides extendido tiene una complejidad cúbica.

# Técnicas de Optimización

- La optimización de estas operaciones se realiza en tres campos fundamentales:

# Técnicas de Optimización

- La optimización de estas operaciones se realiza en tres campos fundamentales:
  - Eliminación del cálculo de inversos siempre que sea posible, cambiándolas por multiplicaciones. Para ello se utilizan coordenadas proyectivas y es posible dejar el número de inversos exclusivamente en uno para normalizar el resultado final.

# Técnicas de Optimización

- La optimización de estas operaciones se realiza en tres campos fundamentales:
  - Eliminación del cálculo de inversos siempre que sea posible, cambiándolas por multiplicaciones. Para ello se utilizan coordenadas proyectivas y es posible dejar el número de inversos exclusivamente en uno para normalizar el resultado final.
  - Reducción del número de multiplicaciones dentro de lo posible, para ello se utilizan representaciones proyectivas de distinto tipo, como por ejemplo las coordenadas jacobianas. También se puede optimizar utilizando representación NAF o técnicas de ventana o de ventana deslizante.

# Técnicas de Optimización

- La optimización de estas operaciones se realiza en tres campos fundamentales:
  - Eliminación del cálculo de inversos siempre que sea posible, cambiándolas por multiplicaciones. Para ello se utilizan coordenadas proyectivas y es posible dejar el número de inversos exclusivamente en uno para normalizar el resultado final.
  - Reducción del número de multiplicaciones dentro de lo posible, para ello se utilizan representaciones proyectivas de distinto tipo, como por ejemplo las coordenadas jacobianas. También se puede optimizar utilizando representación NAF o técnicas de ventana o de ventana deslizante.
  - Aceleración del algoritmo de multiplicación. En este campo hay mucho trabajo realizado, pero no lo trataremos en este curso.

# Acumulación de Denominadores

- La razón fundamental para la utilización de coordenadas proyectivas es la eliminación del cálculo de inversos modulares.

# Acumulación de Denominadores

- La razón fundamental para la utilización de coordenadas proyectivas es la eliminación del cálculo de inversos modulares.
- Puesto que tenemos que representar puntos del espacio proyectivo, podemos usar coordenadas $(X : Y : Z)$ con la relación de equivalencia de que $(X : Y : Z) = (X' : Y' : Z')$ si y sólo si existe $\mu \in K$ tal que $X = \mu X', Y = \mu Y', Z = \mu Z'$.

# Acumulación de Denominadores

- La razón fundamental para la utilización de coordenadas proyectivas es la eliminación del cálculo de inversos modulares.
- Puesto que tenemos que representar puntos del espacio proyectivo, podemos usar coordenadas $(X : Y : Z)$ con la relación de equivalencia de que $(X : Y : Z) = (X' : Y' : Z')$ si y sólo si existe $\mu \in K$ tal que $X = \mu X', Y = \mu Y', Z = \mu Z'$.
- De esta forma si tenemos que dividir $X$ ó $Y$ por un valor $\alpha$ podemos en su lugar multiplicar $Z$ por la misma cantidad ya que

$$(X/\alpha : Y : Z) = (X : \alpha Y : \alpha Z)$$

# Acumulación de Denominadores

- La razón fundamental para la utilización de coordenadas proyectivas es la eliminación del cálculo de inversos modulares.
- Puesto que tenemos que representar puntos del espacio proyectivo, podemos usar coordenadas $(X : Y : Z)$ con la relación de equivalencia de que $(X : Y : Z) = (X' : Y' : Z')$ si y sólo si existe $\mu \in K$ tal que $X = \mu X', Y = \mu Y', Z = \mu Z'$.
- De esta forma si tenemos que dividir $X$ ó $Y$ por un valor $\alpha$ podemos en su lugar multiplicar $Z$ por la misma cantidad ya que

$$(X/\alpha : Y : Z) = (X : \alpha Y : \alpha Z)$$

- Las coordenadas proyectivas del punto están bien definidas y únicamente tendremos que dividir por la tercera coordenada al final del cómputo $kP$ para obtener la normalización y por tanto, las coordenadas afines.

# Ejemplo I

- Vamos a ver cómo se utilizaría esta técnica para calcular la suma de puntos $A + A$ utilizando como base las fórmulas en representación afín. Si $A = (x_1, y_1)$ debemos calcular

$$m = \frac{3x_1^2 + a}{2y_1} \quad x_3 = -2x_1 + m^2 \quad y_3 = -y_1 + m(x_1 - x_3)$$

# Ejemplo I

- Vamos a ver cómo se utilizaría esta técnica para calcular la suma de puntos $A + A$ utilizando como base las fórmulas en representación afín. Si $A = (x_1, y_1)$ debemos calcular

$$m = \frac{3x_1^2 + a}{2y_1} \quad x_3 = -2x_1 + m^2 \quad y_3 = -y_1 + m(x_1 - x_3)$$

- Supondremos que el punto $A$ está en coordenadad proyectivas $(X_1 : Y_1 : Z_1)$ por lo que $x_1 = \frac{X_1}{Z_1}$ e $y_1 = \frac{Y_1}{Z_1}$.

# Ejemplo I

- Vamos a ver cómo se utilizaría esta técnica para calcular la suma de puntos $A + A$ utilizando como base las fórmulas en representación afín. Si $A = (x_1, y_1)$ debemos calcular

$$m = \frac{3x_1^2 + a}{2y_1} \quad x_3 = -2x_1 + m^2 \quad y_3 = -y_1 + m(x_1 - x_3)$$

- Supondremos que el punto $A$ está en coordenadad proyectivas $(X_1 : Y_1 : Z_1)$ por lo que $x_1 = \frac{X_1}{Z_1}$ e $y_1 = \frac{Y_1}{Z_1}$.
- De ahí obtenemos que $m$ es

$$m = \frac{3x_1^2 + a}{2y_1} = \frac{3\frac{X_1^2}{Z_1^2} + a}{2\frac{Y_1}{Z_1}} = \frac{3X_1^2 + aZ_1^2}{2Y_1Z_1}$$

# Ejemplo II

$$x_3 = -2x_1 + m^2 = -2\frac{X_1}{Z_1} + \frac{\left(3X_1^2 + aZ_1^2\right)^2}{4Y_1^2 Z_1^2} = \frac{-8X_1 Y_1^2 Z_1 + \left(3X_1^2 + aZ_1^2\right)^2}{4Y_1^2 Z_1^2}$$

# Ejemplo II

$$x_3 = -2x_1 + m^2 = -2\frac{X_1}{Z_1} + \frac{\left(3X_1^2 + aZ_1^2\right)^2}{4Y_1^2Z_1^2} = \frac{-8X_1Y_1^2Z_1 + \left(3X_1^2 + aZ_1^2\right)^2}{4Y_1^2Z_1^2}$$

$$y_3 = -y_1 + m(x_1 - x_3) = -\frac{Y_1}{Z_1} + \frac{3X_1^2 + aZ_1^2}{2Y_1Z_1} \cdot \frac{24X_1^2Y_1^2Z_1 - \left(3X_1^2 + aZ_1^2\right)^2}{4Y_1^2Z_1^2} =$$

$$\frac{-8Y_1^4Z_1^2 + 24X_1^2Y_1^2Z_1\left(3X_1^2 + aZ_1^2\right) - \left(3X_1^2 + aZ_1^2\right)^3}{8Y_1^3Z_1^3}$$

# Ejemplo III

Finalmente tenemos que poner el resultado en coordenadas proyectivas eliminando las divisiones, para ello escribiremos $x_3 = \frac{X_3}{Z_3}$ e $y_3 = \frac{Y_3}{Z_3}$. Debemos poner un denominador común que seleccionaremos como $Z_3$. Esto lo podemos hacer multiplicando el numerador y denominador de $x_3$ por $2Y_1Z_1$.

# Ejemplo III

Finalmente tenemos que poner el resultado en coordenadas proyectivas eliminando las divisiones, para ello escribiremos $x_3 = \frac{X_3}{Z_3}$ e $y_3 = \frac{Y_3}{Z_3}$. Debemos poner un denominador común que seleccionaremos como $Z_3$. Esto lo podemos hacer multiplicando el numerador y denominador de $x_3$ por $2Y_1Z_1$.

$$x_3 = \frac{X_3}{Z_3} = \frac{2Y_1Z_1}{2Y_1Z_1} \cdot \frac{-8X_1Y_1^2Z_1 + \left(3X_1^2 + aZ_1^2\right)^2}{4Y_1^2Z_1^2}$$

# Ejemplo III

Finalmente tenemos que poner el resultado en coordenadas proyectivas eliminando las divisiones, para ello escribiremos $x_3 = \frac{X_3}{Z_3}$ e $y_3 = \frac{Y_3}{Z_3}$. Debemos poner un denominador común que seleccionaremos como $Z_3$. Esto lo podemos hacer multiplicando el numerador y denominador de $x_3$ por $2Y_1Z_1$.

$$x_3 = \frac{X_3}{Z_3} = \frac{2Y_1Z_1}{2Y_1Z_1} \cdot \frac{-8X_1Y_1^2Z_1 + \left(3X_1^2 + aZ_1^2\right)^2}{4Y_1^2Z_1^2}$$

$$y_3 = \frac{Y_3}{Z_3} = \frac{-8Y_1^4Z_1^2 + 24X_1^2Y_1^2Z_1\left(3X_1^2 + aZ_1^2\right) - \left(3X_1^2 + aZ_1^2\right)^3}{8Y_1^3Z_1^3}$$

# Ejemplo IV

- De ahí podemos tomar:

# Ejemplo IV

- De ahí podemos tomar:
  - $X_3 = 2Y_1Z_1(-8X_1Y_1^2Z_1 + (3X_1^2 + aZ_1^2)^2)$

# Ejemplo IV

- De ahí podemos tomar:
  - $X_3 = 2Y_1Z_1(-8X_1Y_1^2Z_1 + \left(3X_1^2 + aZ_1^2\right)^2)$
  - $Y_3 = -8Y_1^4Z_1^2 + 24X_1^2Y_1^2Z_1\left(3X_1^2 + aZ_1^2\right) - \left(3X_1^2 + aZ_1^2\right)^3$

# Ejemplo IV

- De ahí podemos tomar:
  - $X_3 = 2Y_1Z_1(-8X_1Y_1^2Z_1 + \left(3X_1^2 + aZ_1^2\right)^2)$
  - $Y_3 = -8Y_1^4Z_1^2 + 24X_1^2Y_1^2Z_1\left(3X_1^2 + aZ_1^2\right) - \left(3X_1^2 + aZ_1^2\right)^3$
  - $Z_3 = 8Y_1^3Z_1^3$

# Ejemplo IV

- De ahí podemos tomar:
  - $X_3 = 2Y_1Z_1(-8X_1Y_1^2Z_1 + (3X_1^2 + aZ_1^2)^2)$
  - $Y_3 = -8Y_1^4Z_1^2 + 24X_1^2Y_1^2Z_1(3X_1^2 + aZ_1^2) - (3X_1^2 + aZ_1^2)^3$
  - $Z_3 = 8Y_1^3Z_1^3$
- El punto viene perfectamente definido en coordenadas proyectivas sin haber sido necesario hacer ningún cálculo de inversos modulares.

# Reducción a Operaciones Básicas

- El cálculo que hemos realizado de $X_3$, $Y_3$ y $Z_3$ debe reducirse a una serie de sumas y multiplicaciones.

# Reducción a Operaciones Básicas

- El cálculo que hemos realizado de $X_3$, $Y_3$ y $Z_3$ debe reducirse a una serie de sumas y multiplicaciones.
- Tanto la suma y la multiplicación se implementan como operaciones binarias, por lo que hay que reducir el cálculo a una serie de sumas y productos de sólo dos términos.

# Reducción a Operaciones Básicas

- El cálculo que hemos realizado de $X_3$, $Y_3$ y $Z_3$ debe reducirse a una serie de sumas y multiplicaciones.
- Tanto la suma y la multiplicación se implementan como operaciones binarias, por lo que hay que reducir el cálculo a una serie de sumas y productos de sólo dos términos.
- La forma de hacerlo de un modo óptimo es objeto de investigación y podemos encontrar un listado exhaustivo en `https://hyperelliptic.org/EFD/g1p/auto-shortw-projective.html`.

# Reducción a Operaciones Básicas

- El cálculo que hemos realizado de $X_3$, $Y_3$ y $Z_3$ debe reducirse a una serie de sumas y multiplicaciones.
- Tanto la suma y la multiplicación se implementan como operaciones binarias, por lo que hay que reducir el cálculo a una serie de sumas y productos de sólo dos términos.
- La forma de hacerlo de un modo óptimo es objeto de investigación y podemos encontrar un listado exhaustivo en `https://hyperelliptic.org/EFD/g1p/auto-shortw-projective.html`.
- Vamos a ver una de dichas formas descrita en dicha página web y procedente de la publicación: *1998 Cohen–Miyaji–Ono "Efficient elliptic curve exponentiation using mixed coordinates"*.

**Cálculo de** $(X_3 : Y_3 : Z_3) = 2Acum$ **con** $Acum = (X_1 : Y_1 : Z_1)$**.**

```
w = a*Z1^2+3*X1^2
s = Y1*Z1
ss = s^2
sss = s*ss
R = Y1*s
B = X1*R
h = w2-8*B
X3 = 2*h*s
Y3 = w*(4*B-h)-8*R^2
Z3 = 8*sss
```

Total: 11 multiplicaciones, junto con sumas y productos por constantes (que se pueden programar de forma mucho más eficiente).

# Algoritmo de Multiplicación Escalar

- El algoritmo de multiplicación escalar para el cálculo de $kP$ requiere un acumulador que sumaremos consigo mismo y también la suma de ese acumulador con $P$.

# Algoritmo de Multiplicación Escalar

- El algoritmo de multiplicación escalar para el cálculo de $kP$ requiere un acumulador que sumaremos consigo mismo y también la suma de ese acumulador con $P$.
- Ya hemos visto como hacer la operación $2Acum$, para hacer la operación $Acum = Acum + P$ el punto $P$ podemos suponer que está en forma afín, ya que es siempre el mismo y es el que recibimos para aplicar el algoritmo.

# Algoritmo de Multiplicación Escalar

- El algoritmo de multiplicación escalar para el cálculo de $kP$ requiere un acumulador que sumaremos consigo mismo y también la suma de ese acumulador con $P$.
- Ya hemos visto como hacer la operación $2Acum$, para hacer la operación $Acum = Acum + P$ el punto $P$ podemos suponer que está en forma afín, ya que es siempre el mismo y es el que recibimos para aplicar el algoritmo.
- Por eso tomaremos $P = (X_2 : Y_2 : 1)$.

# Algoritmo de Multiplicación Escalar

- El algoritmo de multiplicación escalar para el cálculo de $kP$ requiere un acumulador que sumaremos consigo mismo y también la suma de ese acumulador con $P$.
- Ya hemos visto como hacer la operación $2Acum$, para hacer la operación $Acum = Acum + P$ el punto $P$ podemos suponer que está en forma afín, ya que es siempre el mismo y es el que recibimos para aplicar el algoritmo.
- Por eso tomaremos $P = (X_2 : Y_2 : 1)$.
- Al finalizar el algoritmo, el resultado final $(X : Y : Z)$ tendremos que normalizarlo, para ello calcularemos un inverso modular $Z^{-1}$ y con dos multiplicaciones $(X * Z^{-1}, Y * Z^{-1})$ obtenemos el resultado final en coordenadas afines.

**Cálculo de $(X_3 : Y_3 : Z_3) = Acum + P$ con $Acum = (X_1 : Y_1 : Z_1)$, $P = (X_2 : Y_2 : 1)$.**

```
u = Y2*Z1-Y1
uu = u^2
v = X2*Z1-X1
vv = v^2
vvv = v*vv
R = vv*X1
A = uu*Z1-vvv-2*R
X3 = v*A
Y3 = u*(R-A)-vvv*Y1
Z3 = vvv*Z1
```

Total: 11 multiplicaciones, junto con sumas y productos por constantes.

# Otras Coordenadas Proyectivas

- Hemos utilizado las coordenadas proyectivas $(X : Y : Z)$ para representar el punto afín $(X/Z, Y/Z)$.

# Otras Coordenadas Proyectivas

- Hemos utilizado las coordenadas proyectivas $(X : Y : Z)$ para representar el punto afín $(X/Z, Y/Z)$.
- Se han estudiado otros tipos de coordenadas que optimizan las operaciones criptográficas.

# Otras Coordenadas Proyectivas

- Hemos utilizado las coordenadas proyectivas $(X : Y : Z)$ para representar el punto afín $(X/Z, Y/Z)$.
- Se han estudiado otros tipos de coordenadas que optimizan las operaciones criptográficas.
- Concretamente, podemos utilizar las llamadas coordenadas Jacobianas, en las que con los tres valores $(X : Y : Z)$ representamos el punto afín $(X/Z^2, Y/Z^3)$.

# Otras Coordenadas Proyectivas

- Hemos utilizado las coordenadas proyectivas $(X : Y : Z)$ para representar el punto afín $(X/Z, Y/Z)$.
- Se han estudiado otros tipos de coordenadas que optimizan las operaciones criptográficas.
- Concretamente, podemos utilizar las llamadas coordenadas Jacobianas, en las que con los tres valores $(X : Y : Z)$ representamos el punto afín $(X/Z^2, Y/Z^3)$.
- Si $Z = 1$ el punto en coordenadas jacobianas $(x : y : 1)$ es el punto afín $(x, y)$.

# Otras Coordenadas Proyectivas

- Hemos utilizado las coordenadas proyectivas $(X : Y : Z)$ para representar el punto afín $(X/Z, Y/Z)$.
- Se han estudiado otros tipos de coordenadas que optimizan las operaciones criptográficas.
- Concretamente, podemos utilizar las llamadas coordenadas Jacobianas, en las que con los tres valores $(X : Y : Z)$ representamos el punto afín $(X/Z^2, Y/Z^3)$.
- Si $Z = 1$ el punto en coordenadas jacobianas $(x : y : 1)$ es el punto afín $(x, y)$.
- Las fórmulas que vamos a ver a continuación proceden de `https://hyperelliptic.org/EFD/g1p/auto-shortw-jacobian.html`

## Cálculo de $(X_3 : Y_3 : Z_3) = 2Acum$ con $Acum = (X_1 : Y_1 : Z_1)$ en coordenadas Jacobianas.

```
XX = X1^2
YY = Y1^2
ZZ = Z1^2
S = 4*X1*YY
M = 3*XX+a*ZZ^2
T = M^2-2*S
X3 = T
Y3 = M*(S-T)-8*YY^2
Z3 = 2*Y1*Z1
```

Total: 9 multiplicaciones, junto con sumas y productos por constantes (que se pueden programar de forma mucho más eficiente).

## Cálculo de $(X_3 : Y_3 : Z_3) = Acum + P$ con $Acum = (X_1 : Y_1 : Z_1)$, $P = (X_2 : Y_2 : 1)$ en coordenadas Jabocianas.

```
Z1Z1 = Z1^2
U2 = X2*Z1Z1
S2 = Y2*Z1*Z1Z1
H = U2-X1
HH = H^2
I = 4*HH
J = H*I
r = 2*(S2-Y1)
V = X1*I
X3 = r^2-J-2*V
Y3 = r*(V-X3)-2*Y1*J
Z3 = (Z1+H)^2-Z1Z1-HH
```

Total: 11 multiplicaciones, junto con sumas y productos por constantes.

# Comentarios Finales

- En el caso particular en que $a$ sea $-3$ es posible hacer la operación $2Acum$ con una multiplicación menos, reordenando las operaciones. Por eso se suelen buscar curvas con ese parámetro especial.

# Comentarios Finales

- En el caso particular en que $a$ sea $-3$ es posible hacer la operación $2Acum$ con una multiplicación menos, reordenando las operaciones. Por eso se suelen buscar curvas con ese parámetro especial.
- Una vez que se ha calculado el resultado en coordenadas jacobianas $(X : Y : Z)$ se calculará un inverso modular $Z^{-1}$ y cuatro multiplicaciones obtenemos $x = X * (Z^{-1})^2$, $y = Y * (Z^{-1})^3$, que es el resultado final en coordenadas afines.