MOOC de Criptología Matemática. Curvas Elípticas

Leandro Marín

Módulo III. Sesión 2.
Dificultad Alta

Definición

Curva Elíptica

Sea K un cuerpo, una curva elíptica E sobre K es una curva cúbica irreducible en el plano proyectivo no degenerada junto con un punto O de la curva en el plano proyectivo $\mathbb{P}^2(K)$.

Puntos Racionales

- Sea E una curva elíptica sobre K, a los puntos del plano proyectivo $\mathbb{P}^2(K)$ que satisfacen la ecuación del la curva los llamaremos puntos racionales. El conjunto de puntos racionales de E sobre el cuerpo K se denotará $E(K)$.

Puntos Racionales

- Sea E una curva elíptica sobre K, a los puntos del plano proyectivo $\mathbb{P}^2(K)$ que satisfacen la ecuación del la curva los llamaremos puntos racionales. El conjunto de puntos racionales de E sobre el cuerpo K se denotará $E(K)$.
- Por definición sabemos que este conjunto no puede ser vacío porque el punto O cumple las condiciones de ser un punto racional.

Puntos Racionales

- Sea E una curva elíptica sobre K, a los puntos del plano proyectivo $\mathbb{P}^2(K)$ que satisfacen la ecuación del la curva los llamaremos puntos racionales. El conjunto de puntos racionales de E sobre el cuerpo K se denotará $E(K)$.
- Por definición sabemos que este conjunto no puede ser vacío porque el punto O cumple las condiciones de ser un punto racional.
- Los puntos racionales de la curva serán los que utilicemos para representar la información que se usa en los protocolos criptográficos sobre curvas elípticas.

Puntos Racionales

- Sea E una curva elíptica sobre K, a los puntos del plano proyectivo $\mathbb{P}^2(K)$ que satisfacen la ecuación del la curva los llamaremos puntos racionales. El conjunto de puntos racionales de E sobre el cuerpo K se denotará $E(K)$.
- Por definición sabemos que este conjunto no puede ser vacío porque el punto O cumple las condiciones de ser un punto racional.
- Los puntos racionales de la curva serán los que utilicemos para representar la información que se usa en los protocolos criptográficos sobre curvas elípticas.
- Cuando nos proporcionen una curva para usarla en criptografía, uno de los parámetros que se nos dará será el número exacto de puntos racionales que contiene.

Estructura de Grupo

- El conjunto de puntos racionales de una curva elíptica puede ser dotado de una operación $+$ de tal forma que cumple las propiedades de grupo abeliano.

Estructura de Grupo

- El conjunto de puntos racionales de una curva elíptica puede ser dotado de una operación $+$ de tal forma que cumple las propiedades de grupo abeliano.
- Es decir, se cumplen las siguientes propiedades:

Estructura de Grupo

- El conjunto de puntos racionales de una curva elíptica puede ser dotado de una operación $+$ de tal forma que cumple las propiedades de grupo abeliano.
- Es decir, se cumplen las siguientes propiedades:
  - $(P + Q) + R = P + (Q + R)$ para todo $P, Q, R \in E(K)$

Estructura de Grupo

- El conjunto de puntos racionales de una curva elíptica puede ser dotado de una operación $+$ de tal forma que cumple las propiedades de grupo abeliano.
- Es decir, se cumplen las siguientes propiedades:
  - $(P + Q) + R = P + (Q + R)$ para todo $P, Q, R \in E(K)$
  - $P + Q = Q + P$ para todo $P, Q \in E(K)$

Estructura de Grupo

- El conjunto de puntos racionales de una curva elíptica puede ser dotado de una operación $+$ de tal forma que cumple las propiedades de grupo abeliano.
- Es decir, se cumplen las siguientes propiedades:
  - $(P + Q) + R = P + (Q + R)$ para todo $P, Q, R \in E(K)$
  - $P + Q = Q + P$ para todo $P, Q \in E(K)$
  - $P + O = P$ para todo $P \in E(K)$

Estructura de Grupo

- El conjunto de puntos racionales de una curva elíptica puede ser dotado de una operación $+$ de tal forma que cumple las propiedades de grupo abeliano.
- Es decir, se cumplen las siguientes propiedades:
  - $(P+Q)+R = P+(Q+R)$ para todo $P, Q, R \in E(K)$
  - $P+Q = Q+P$ para todo $P, Q \in E(K)$
  - $P+O = P$ para todo $P \in E(K)$
  - Para todo $P \in E(K)$ existe $-P \in E(K)$ tal que $P+(-P) = O$.

Estructura de Grupo

- El conjunto de puntos racionales de una curva elíptica puede ser dotado de una operación $+$ de tal forma que cumple las propiedades de grupo abeliano.
- Es decir, se cumplen las siguientes propiedades:
  - $(P+Q)+R = P+(Q+R)$ para todo $P, Q, R \in E(K)$
  - $P+Q = Q+P$ para todo $P, Q \in E(K)$
  - $P+O = P$ para todo $P \in E(K)$
  - Para todo $P \in E(K)$ existe $-P \in E(K)$ tal que $P+(-P) = O$.
- La definición exacta de la operación $+$ la veremos más adelante.

Estructura de Grupo

- El conjunto de puntos racionales de una curva elíptica puede ser dotado de una operación $+$ de tal forma que cumple las propiedades de grupo abeliano.
- Es decir, se cumplen las siguientes propiedades:
  - $(P+Q)+R = P+(Q+R)$ para todo $P, Q, R \in E(K)$
  - $P+Q = Q+P$ para todo $P, Q \in E(K)$
  - $P+O = P$ para todo $P \in E(K)$
  - Para todo $P \in E(K)$ existe $-P \in E(K)$ tal que $P+(-P) = O$.
- La definición exacta de la operación $+$ la veremos más adelante.
- Esta operación es la que se usará en los protocolos criptográficos.

Ejemplo

- Antes de seguir adelante analizando la definición, vamos a ver un ejemplo.

Ejemplo

- Antes de seguir adelante analizando la definición, vamos a ver un ejemplo.
- Consideremos la curva $y^2 = x^3 + 2x + 1$ sobre el cuerpo $K = \mathbb{Z}_5$.

Ejemplo

- Antes de seguir adelante analizando la definición, vamos a ver un ejemplo.
- Consideremos la curva $y^2 = x^3 + 2x + 1$ sobre el cuerpo $K = \mathbb{Z}_5$.
- Esta es una curva en el plano afín y podemos ver que los puntos (x, y) que pertenecen a la curva son los siguientes:

$$\{(0,1),(0,4),(1,2),(1,3),(3,2),(3,3)\}$$

Ejemplo

- Antes de seguir adelante analizando la definición, vamos a ver un ejemplo.
- Consideremos la curva $y^2 = x^3 + 2x + 1$ sobre el cuerpo $K = \mathbb{Z}_5$.
- Esta es una curva en el plano afín y podemos ver que los puntos (x, y) que pertenecen a la curva son los siguientes:

$$\{(0,1),(0,4),(1,2),(1,3),(3,2),(3,3)\}$$

- La curva la debemos considerar en el plano proyectivo, por lo que necesitamos calcular los puntos del infinito, si los tuviera.

Puntos del infinito

- Tal y como hacíamos en la sesión anterior, debemos calcular la fórmula de la curva en su forma homogénea. Para ello debemos poner $y = \frac{Y}{Z}$, $x = \frac{X}{Z}$ y eliminar denominadores multiplicando por Z^3, con lo que nos queda la fórmula

$$Y^2Z = X^3 + 2XZ^2 + Z^3$$

Puntos del infinito

- Tal y como hacíamos en la sesión anterior, debemos calcular la fórmula de la curva en su forma homogénea. Para ello debemos poner $y = \frac{Y}{Z}$, $x = \frac{X}{Z}$ y eliminar denominadores multiplicando por Z^3, con lo que nos queda la fórmula

$$Y^2Z = X^3 + 2XZ^2 + Z^3$$

- Si hacemos $Z = 0$ obtenemos $0 = X^3$ y por lo tanto $X = 0$, lo que nos deja como punto del infinito el correspondiente a $(0 : Y : 0)$ con $Y \in K \setminus \{0\}$.

Puntos del infinito

- Tal y como hacíamos en la sesión anterior, debemos calcular la fórmula de la curva en su forma homogénea. Para ello debemos poner $y = \frac{Y}{Z}$, $x = \frac{X}{Z}$ y eliminar denominadores multiplicando por Z^3, con lo que nos queda la fórmula

$$Y^2Z = X^3 + 2XZ^2 + Z^3$$

- Si hacemos $Z = 0$ obtenemos $0 = X^3$ y por lo tanto $X = 0$, lo que nos deja como punto del infinito el correspondiente a $(0 : Y : 0)$ con $Y \in K \setminus \{0\}$.
- En coordenadas proyectivas este punto es el mismo que $(0 : 1 : 0)$ y es el único punto del infinito de esta curva.

Puntos del infinito

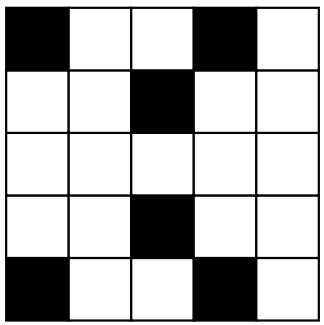
- Tal y como hacíamos en la sesión anterior, debemos calcular la fórmula de la curva en su forma homogénea. Para ello debemos poner $y = \frac{Y}{Z}$, $x = \frac{X}{Z}$ y eliminar denominadores multiplicando por Z^3, con lo que nos queda la fórmula

$$Y^2Z = X^3 + 2XZ^2 + Z^3$$

- Si hacemos $Z = 0$ obtenemos $0 = X^3$ y por lo tanto $X = 0$, lo que nos deja como punto del infinito el correspondiente a $(0 : Y : 0)$ con $Y \in K \setminus \{0\}$.
- En coordenadas proyectivas este punto es el mismo que $(0 : 1 : 0)$ y es el único punto del infinito de esta curva.
- Vamos a tomar como punto O en la definición de curva elíptica precisamente este punto proyectivo.

Curva Elíptica $y^2 = x^3 + 2x + 1$

La representación gráfica de los puntos afines de esta curva elíptica sería la siguiente:



Estructura de Grupo

- El número total de puntos en nuestra curva es de 7, de los cuales 6 están en el plano afín y uno (el punto O) en la recta del infinito.

Estructura de Grupo

- El número total de puntos en nuestra curva es de 7, de los cuales 6 están en el plano afín y uno (el punto O) en la recta del infinito.
- Por definición, $P + O = P = O + P$ por lo que sólo necesitamos conocer la suma de puntos $P + Q$ cuando P y Q sean ambos distintos de O.

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

Grupos Cíclicos

- Al tratarse de un grupo con un número primo de elementos, 7, podemos estar seguros de que es un grupo cíclico.

Grupos Cíclicos

- Al tratarse de un grupo con un número primo de elementos, 7, podemos estar seguros de que es un grupo cíclico.
- Esto significa que si denotamos $0P = O$, $1P = P$, $2P = P + P$, $3P = P + P + P$, etc podemos garantizar que existe un punto G tal que todos los demás puntos son de la forma kG para algún valor de k.

Grupos Cíclicos

- Al tratarse de un grupo con un número primo de elementos, 7, podemos estar seguros de que es un grupo cíclico.
- Esto significa que si denotamos $0P = O$, $1P = P$, $2P = P + P$, $3P = P + P + P$, etc podemos garantizar que existe un punto G tal que todos los demás puntos son de la forma kG para algún valor de k.
- A un elemento G de esta forma se le conoce como un generador del grupo.

Grupos Cíclicos

- Al tratarse de un grupo con un número primo de elementos, 7, podemos estar seguros de que es un grupo cíclico.
- Esto significa que si denotamos $0P = O$, $1P = P$, $2P = P + P$, $3P = P + P + P$, etc podemos garantizar que existe un punto G tal que todos los demás puntos son de la forma kG para algún valor de k.
- A un elemento G de esta forma se le conoce como un generador del grupo.
- En realidad, cualquier elemento distinto de O es un generador de este grupo, vamos a verlo.

Generadores

- Tomemos como G por ejemplo $(0, 1)$.

Generadores

- Tomemos como G por ejemplo $(0, 1)$.
- Utilizando la tabla de operaciones del grupo, podemo ver que
  $2G = (0, 1) + (0, 1) = (1, 3)$,
  $3G = 2G + G = (1, 3) + (0, 1) = (3, 3)$,
  $4G = 3G + G = (3, 3) + (0, 1) = (3, 2)$,
  $5G = 4G + G = (3, 2) + (0, 1) = (1, 2)$,
  $6G = 5G + G = (1, 2) + (0, 1) = (0, 4)$ y
  $7G = 6G + G = (0, 4) + (0, 1) = O$.

Generadores

- Tomemos como G por ejemplo $(0, 1)$.
- Utilizando la tabla de operaciones del grupo, podemo ver que
  $2G = (0, 1) + (0, 1) = (1, 3)$,
  $3G = 2G + G = (1, 3) + (0, 1) = (3, 3)$,
  $4G = 3G + G = (3, 3) + (0, 1) = (3, 2)$,
  $5G = 4G + G = (3, 2) + (0, 1) = (1, 2)$,
  $6G = 5G + G = (1, 2) + (0, 1) = (0, 4)$ y
  $7G = 6G + G = (0, 4) + (0, 1) = O$.
- A partir de ahí todos los elementos se repiten, puesto que $(k + 7)G = kG + 7G = kG + O = kG$ para cualquier k.

Generadores

- Tomemos como G por ejemplo $(0, 1)$.
- Utilizando la tabla de operaciones del grupo, podemo ver que
  $2G = (0, 1) + (0, 1) = (1, 3)$,
  $3G = 2G + G = (1, 3) + (0, 1) = (3, 3)$,
  $4G = 3G + G = (3, 3) + (0, 1) = (3, 2)$,
  $5G = 4G + G = (3, 2) + (0, 1) = (1, 2)$,
  $6G = 5G + G = (1, 2) + (0, 1) = (0, 4)$ y
  $7G = 6G + G = (0, 4) + (0, 1) = O$.
- A partir de ahí todos los elementos se repiten, puesto que $(k + 7)G = kG + 7G = kG + O = kG$ para cualquier k.
- Como podemos ver, utilizar un generador para representar el grupo nos permite decir que los elementos de grupo son $0G, 1G, 2G, 3G, 4G, 5G, 6G$ y la suma $kG + tG = (k + t)G$ con la regla de que si la suma es mayor que 7, podemos restar 7 para dejar el restultado entre $0G$ y $6G$.

Simetría

- Otra propiedad que podemos apreciar en los puntos de la curva $y^2 = x^3 + 2x + 1$ es que si (x, y) es un punto de la curva, $(x, -y)$ también lo es puesto que $y^2 = (-y)^2$.

Simetría

- Otra propiedad que podemos apreciar en los puntos de la curva $y^2 = x^3 + 2x + 1$ es que si (x, y) es un punto de la curva, $(x, -y)$ también lo es puesto que $y^2 = (-y)^2$.
- De esta forma, los puntos distintos de O vienen en pares $\{(0, 1), (0, -1) = (0, 4)\}$, $\{(1, 2), (1, -2) = (1, 3)\}$, $\{(3, 2), (3, -2) = (3, 3)\}$.

Simetría

- Otra propiedad que podemos apreciar en los puntos de la curva $y^2 = x^3 + 2x + 1$ es que si (x, y) es un punto de la curva, $(x, -y)$ también lo es puesto que $y^2 = (-y)^2$.
- De esta forma, los puntos distintos de O vienen en pares $\{(0, 1), (0, -1) = (0, 4)\}$, $\{(1, 2), (1, -2) = (1, 3)\}$, $\{(3, 2), (3, -2) = (3, 3)\}$.
- Además, podemos ver en la tabla que para todos ellos se tiene que $(x, y) + (x, -y) = O$.

Simetría

- Otra propiedad que podemos apreciar en los puntos de la curva $y^2 = x^3 + 2x + 1$ es que si (x, y) es un punto de la curva, $(x, -y)$ también lo es puesto que $y^2 = (-y)^2$.
- De esta forma, los puntos distintos de O vienen en pares $\{(0, 1), (0, -1) = (0, 4)\}$, $\{(1, 2), (1, -2) = (1, 3)\}$, $\{(3, 2), (3, -2) = (3, 3)\}$.
- Además, podemos ver en la tabla que para todos ellos se tiene que $(x, y) + (x, -y) = O$.
- Dicho de otra forma, si $P = (x, y)$, entonces $-P = (x, -y)$ en este grupo.

Forma Normal de Weierstrass

- Dos curvas elípticas que nos proporcionen la misma estructura, en realidad pueden ser consideradas iguales.

Forma Normal de Weierstrass

- Dos curvas elípticas que nos proporcionen la misma estructura, en realidad pueden ser consideradas iguales.
- De esta forma se pueden realizar transformaciones que nos den una forma más simplificada de la curva, siempre que mantengan la estructura de los puntos.

Forma Normal de Weierstrass

- Dos curvas elípticas que nos proporcionen la misma estructura, en realidad pueden ser consideradas iguales.
- De esta forma se pueden realizar transformaciones que nos den una forma más simplificada de la curva, siempre que mantengan la estructura de los puntos.
- Una de las transformaciones que se puede hacer es poner el punto O siempre en en punto del infinito $(0 : 1 : 0)$ tal y como sucedía en el ejemplo.

Forma Normal de Weierstrass

- Dos curvas elípticas que nos proporcionen la misma estructura, en realidad pueden ser consideradas iguales.
- De esta forma se pueden realizar transformaciones que nos den una forma más simplificada de la curva, siempre que mantengan la estructura de los puntos.
- Una de las transformaciones que se puede hacer es poner el punto O siempre en en punto del infinito $(0 : 1 : 0)$ tal y como sucedía en el ejemplo.
- Haciendo otros tipos de transformaciones podemos conseguir que si la característica del cuerpo no es ni 2 ni 3, la curva sea de la forma:

$$y^2 = x^3 + ax + b$$

Forma Normal de Weierstrass

- Dos curvas elípticas que nos proporcionen la misma estructura, en realidad pueden ser consideradas iguales.
- De esta forma se pueden realizar transformaciones que nos den una forma más simplificada de la curva, siempre que mantengan la estructura de los puntos.
- Una de las transformaciones que se puede hacer es poner el punto O siempre en en punto del infinito $(0 : 1 : 0)$ tal y como sucedía en el ejemplo.
- Haciendo otros tipos de transformaciones podemos conseguir que si la característica del cuerpo no es ni 2 ni 3, la curva sea de la forma:

$$y^2 = x^3 + ax + b$$

- Esta es la conocida como forma normal de Weierstrass.

Introducción

- Aunque en principio podríamos usar cualquier cuerpo, vamos a desarrollar la teoría sobre cuerpos del tipo $K = \mathbb{Z}_p$ con p un número primo grande.

Introducción

- Aunque en principio podríamos usar cualquier cuerpo, vamos a desarrollar la teoría sobre cuerpos del tipo $K = \mathbb{Z}_p$ con p un número primo grande.
- Si $p \neq 2$ y $p \neq 3$ podemos utilizar la forma normal de Weierstrass.

Introducción

- Aunque en principio podríamos usar cualquier cuerpo, vamos a desarrollar la teoría sobre cuerpos del tipo $K = \mathbb{Z}_p$ con p un número primo grande.
- Si $p \neq 2$ y $p \neq 3$ podemos utilizar la forma normal de Weierstrass.
- Los parámetros que debemos introducir para definir la curva son precisamente los valores a y b tales que

$$y^2 = x^3 + ax + b$$

Definición de la Curva

- Vamos a introducir el ejemplo $y^2 = x^3 + 2x + 1$ sobre el cuerpo $\mathbb{Z}_5$.

Definición de la Curva

- Vamos a introducir el ejemplo $y^2 = x^3 + 2x + 1$ sobre el cuerpo $\mathbb{Z}_5$.
- Si ponemos

```
E = EllipticCurve(GF(5),[2,1])
E
```

Definición de la Curva

- Vamos a introducir el ejemplo $y^2 = x^3 + 2x + 1$ sobre el cuerpo $\mathbb{Z}_5$.
- Si ponemos

```
E = EllipticCurve(GF(5),[2,1])
E
```

- Nos dirá que `E` es `Elliptic Curve defined by y^2 =x^3 +2*x + 1 over Finite Field of size 5`

Lista de Puntos de `E`

- En las curvas con un número pequeño de puntos, podemos listar todos los puntos con el comando `E.points()`

Lista de Puntos de `E`

- En las curvas con un número pequeño de puntos, podemos listar todos los puntos con el comando `E.points()`
- Este comando nos devolverá la lista:

```
[(0:1:0),(0:1:1),(0:4:1),(1:2:1),(1:3:1),(3:2:1),(3:3:1)]
```

Lista de Puntos de `E`

- En las curvas con un número pequeño de puntos, podemos listar todos los puntos con el comando `E.points()`
- Este comando nos devolverá la lista:

```
[(0:1:0),(0:1:1),(0:4:1),(1:2:1),(1:3:1),(3:2:1),(3:3:1)]
```

- Como podemos ver, empieza dándonos el elemento O que es el punto del infinito (tercera coordenada igual a 0) y luego los puntos afines (tercera coordenada igual a 1).

Lista de Puntos de `E`

- En las curvas con un número pequeño de puntos, podemos listar todos los puntos con el comando `E.points()`
- Este comando nos devolverá la lista:

```
[(0:1:0),(0:1:1),(0:4:1),(1:2:1),(1:3:1),(3:2:1),(3:3:1)]
```

- Como podemos ver, empieza dándonos el elemento O que es el punto del infinito (tercera coordenada igual a 0) y luego los puntos afines (tercera coordenada igual a 1).
- Este comando sólo se puede usar cuando el número de puntos es pequeño.

Número de Puntos de la Curva

- Aunque la lista completa de puntos sólo la podemos obtener para curvas pequeñas, el número total de puntos lo podemos obtener incluso para curvas más grandes.

Número de Puntos de la Curva

- Aunque la lista completa de puntos sólo la podemos obtener para curvas pequeñas, el número total de puntos lo podemos obtener incluso para curvas más grandes.
- Por ejemplo, si tomamos el número primo $p = 200 \cdot 256^{19} - 1$ y la curva $y^2 = x^3 - 3x + 1$ tenemos

```
F = EllipticCurve(GF(200*256^19-1),[-3,1])
F.cardinality()
```

Nos responderá que el número de puntos de esta curva es

```
1141798154164767904846627159019786861331808313817
```

Curvas no singulares

- En la definición de curva elíptica, hemos exigido que la curva sea no singular.

Curvas no singulares

- En la definición de curva elíptica, hemos exigido que la curva sea no singular.
- Esa es una condición técnica que impide la existencia de puntos llamados singulares.

Curvas no singulares

- En la definición de curva elíptica, hemos exigido que la curva sea no singular.
- Esa es una condición técnica que impide la existencia de puntos llamados singulares.
- En estos puntos singulares podríamos no tener una recta tangente a la curva.

Curvas no singulares

- En la definición de curva elíptica, hemos exigido que la curva sea no singular.
- Esa es una condición técnica que impide la existencia de puntos llamados singulares.
- En estos puntos singulares podríamos no tener una recta tangente a la curva.
- La mayoría de las curvas son no singulares, pero para asegurarnos debemos comprobar que el valor $\Delta = -16(4a^3 + 27b^2)$ es distinto de 0 en el cuerpo $\mathbb{Z}_p$.

Curvas no singulares

- En la definición de curva elíptica, hemos exigido que la curva sea no singular.
- Esa es una condición técnica que impide la existencia de puntos llamados singulares.
- En estos puntos singulares podríamos no tener una recta tangente a la curva.
- La mayoría de las curvas son no singulares, pero para asegurarnos debemos comprobar que el valor $\Delta = -16(4a^3 + 27b^2)$ es distinto de 0 en el cuerpo $\mathbb{Z}_p$.
- Este valor recibe el nombre de discriminante. Como $-16 \neq 0$ podemos simplemente comprobar que $4a^3 + 27b^2 \neq 0$.

Ejemplo

- Utilizando estos comandos podemos calcular todas las curvas no singulares para el caso $K = \mathbb{Z}_5$

Ejemplo

- Utilizando estos comandos podemos calcular todas las curvas no singulares para el caso $K = \mathbb{Z}_5$
- Para ello podemos recorrer todos los parámetros posibles a y b que nos den un discriminante no nulo.

```
K = GF(5)
for a in K:
  for b in K:
    if 4*a^3+27*b^2!=0:
      print "Los valores ",[a,b],
      print "generan una curva no singular con",
      print EllipticCurve(K,[a,b]).cardinality(),
      print "puntos."
```

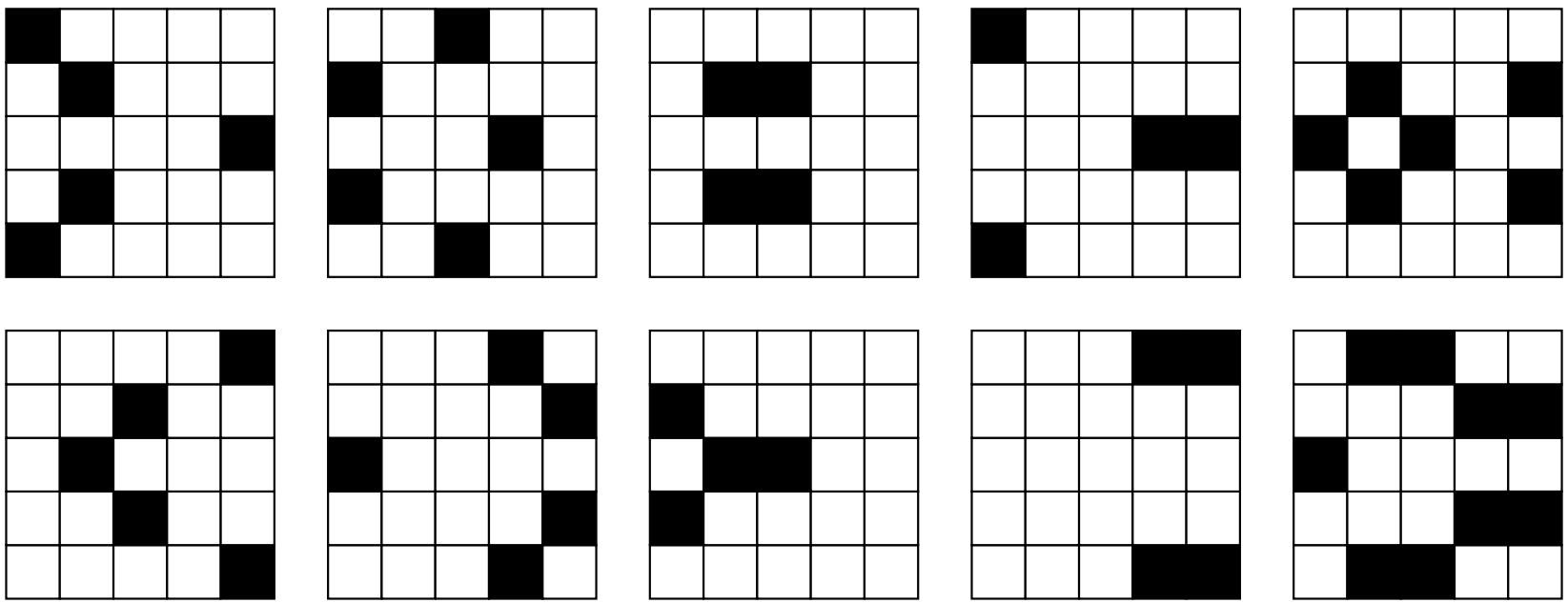
Ejemplo

- Utilizando estos comandos podemos calcular todas las curvas no singulares para el caso $K = \mathbb{Z}_5$
- Para ello podemos recorrer todos los parámetros posibles a y b que nos den un discriminante no nulo.

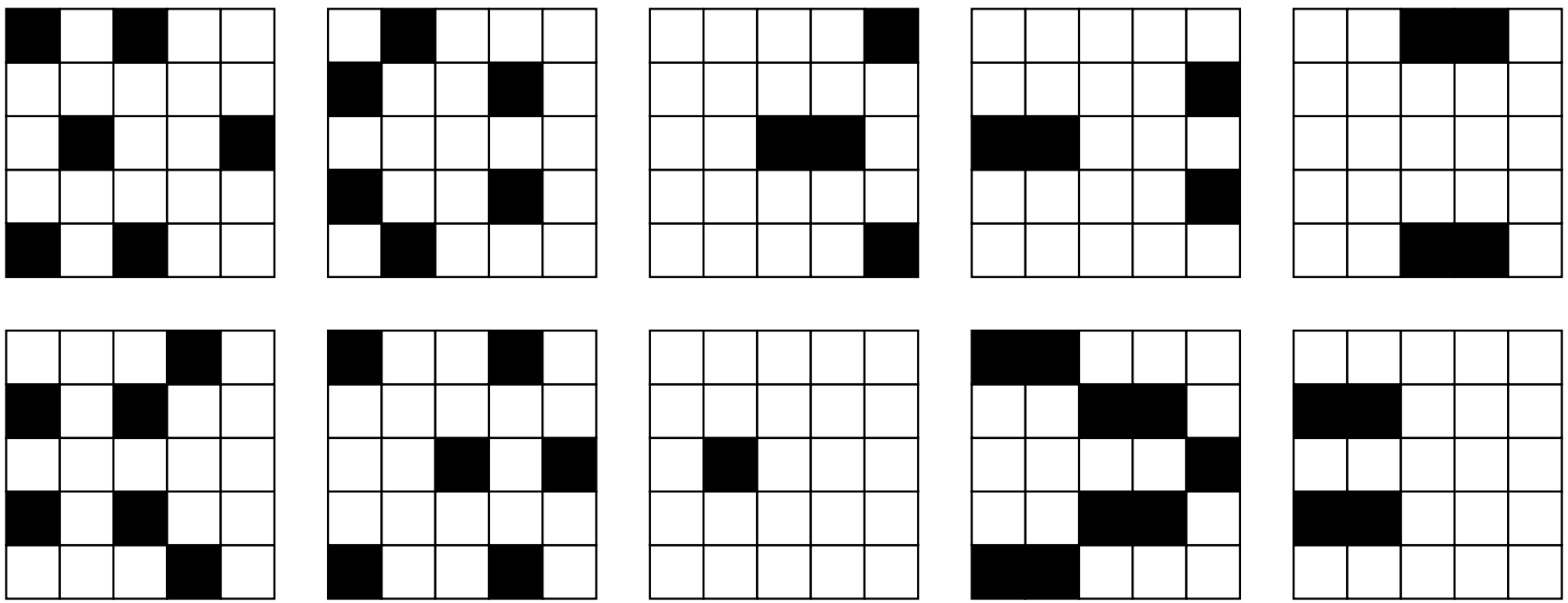
```
K = GF(5)
for a in K:
  for b in K:
    if 4*a^3+27*b^2!=0:
      print "Los valores ",[a,b],
      print "generan una curva no singular con",
      print EllipticCurve(K,[a,b]).cardinality(),
      print "puntos."
```

- Vamos a ver los puntos afines de cada una de ellas representados gráficamente (todas ellas tienen además el punto del infinito $(0 : 1 : 0)$).

Curvas Elípticas no singulares en $\mathbb{P}^2(\mathbb{Z}_5)$ I



Curvas Elípticas no singulares en $\mathbb{P}^2(\mathbb{Z}_5)$ II



Buscando Curvas Válidas I

- Las curvas sobre un cuerpo tan pequeño como $\mathbb{Z}_5$ no son útiles para criptografía.

Buscando Curvas Válidas I

- Las curvas sobre un cuerpo tan pequeño como $\mathbb{Z}_5$ no son útiles para criptografía.
- Aunque normalmente nos darán los parámetros de la curva, podemos necesitar en algún momento obtener una curva válida para usar en algún protocolo.

Buscando Curvas Válidas I

- Las curvas sobre un cuerpo tan pequeño como $\mathbb{Z}_5$ no son útiles para criptografía.
- Aunque normalmente nos darán los parámetros de la curva, podemos necesitar en algún momento obtener una curva válida para usar en algún protocolo.
- Para ello debemos empezar eligiendo un número primo p del tamaño adecuado (entre 160 y 256 bits).

Buscando Curvas Válidas I

- Las curvas sobre un cuerpo tan pequeño como $\mathbb{Z}_5$ no son útiles para criptografía.
- Aunque normalmente nos darán los parámetros de la curva, podemos necesitar en algún momento obtener una curva válida para usar en algún protocolo.
- Para ello debemos empezar eligiendo un número primo p del tamaño adecuado (entre 160 y 256 bits).
- Para saber si un número es primo podemos usar el comando `is_prime(p)`, por ejemplo

```
p = 200*256^19-1
print is_prime(p)
print p.nbits()
```

Nos responderá que este número es efectivamente primo y que tiene 160 bits.

Buscando Curvas Válidas II

- Una vez fijado el primo, debemos buscar valores a y b que nos den una curva no singular y que a su vez tenga un número de puntos primo.

Buscando Curvas Válidas II

- Una vez fijado el primo, debemos buscar valores a y b que nos den una curva no singular y que a su vez tenga un número de puntos primo.
- Para ello simplemente buscaremos valores aleatorios. El valor $a = -3$ tiene algunas ventajas que veremos más adelante. Podemos buscar la curva del siguiente modo:

```
p = 200*256^19-1
K = GF(p)
a = -3
for b in range(300,350):
  if K(4*a*a*a+27*b*b)!=0:
    n = EllipticCurve(K,[a,b]).cardinality()
    if is_prime(n):
      print "Curva a =",a,"b = ",b,"n = ",n
```

Buscando Curvas Válidas II

- Una vez fijado el primo, debemos buscar valores a y b que nos den una curva no singular y que a su vez tenga un número de puntos primo.
- Para ello simplemente buscaremos valores aleatorios. El valor $a = -3$ tiene algunas ventajas que veremos más adelante. Podemos buscar la curva del siguiente modo:

```
p = 200*256^19-1
K = GF(p)
a = -3
for b in range(300,350):
  if K(4*a*a*a+27*b*b)!=0:
    n = EllipticCurve(K,[a,b]).cardinality()
    if is_prime(n):
      print "Curva a =",a,"b = ",b,"n = ",n
```

- Nos responderá

```
Curva a = -3 b =  311
n =  1141798154164767904846627604008953027969948732229
```