Thm: $\mathbb{F}_p$ cuerpo finito.

(a) $\forall d \geq 1$ $\exists$ un polinomio irreducible de grado d.

(b) $\forall d \geq 1$ $\exists$ un cuerpo con p^d elementos

(c) Si $\mathbb{F}$ y $\mathbb{F}'$ finitos con $\#\mathbb{F} = \#\mathbb{F}'$, son isomorfos.

(a) $\mathbb{F}$ con $q = p^d$ elementos. Entonces $\mathbb{F}^\times$ tiene una raíz primitiva.

Ahora regresamos a curvas elípticas:

Thm (Hasse) $E \setminus \mathbb{F}_{p^k}$

$$\Rightarrow \#E(\mathbb{F}_{p^k}) = p^k + 1 - t_{p^k} \quad \text{con} \quad |t_{p^k}| \leq 2p^{k/2}$$

Eg: $\mathbb{F}_q = \mathbb{F}_3[x]/(x^2+1)$ (o sea $\mathbb{F}_q = \{a+bi : a,b \in \mathbb{F}_3\}$ con $i^2+1=0$)

Sea $E: Y^2 = X^3 + (1+i)X + (2+i)$

Hay 10 puntos. $(2,0) \in E(\mathbb{F}_q)$: $0^2 = 2^3 + 2+2i+2+i$

$= 12 + 3i$ los coeficientes están en $\mathbb{F}_3$

$= 0$ porque

Usando las fórmulas como antes se puede sumar y doblar puntos, y siempre teniendo en cuenta que los coefs son $0, 1, 2$ módulo 3 e $i^2 = -1$

Queremos definir curvas elípticas en $\mathbb{F}_{2^k}$ pero antes hicimos una trampa

De hecho Δ no es $4A^3+27B^2$ pero sí $\Delta = -16(4A^3+27B^2)$

La condición $\Delta \neq 0$ nunca se va a cumplir en $\mathbb{F}_{2^k}$.

También no necesariamente se puede tiene que escribir como $Y^2 = X^3 + AX + B$

~~método 2 porque se~~

Def Una curva elíptica E es el conjunto de soluciones a una ecuación Weierstrass generalizada:

$$E: Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

(X tiene peso 2 e Y peso 3; cada monomio tiene peso 6.)

a_i peso i.

Obs: • Existe expresión para $\Delta = \Delta(a_1, a_2, a_3, a_4, a_6)$

$\Delta \neq 0 \iff E$ no singular

• La operación es lo mismo menos el reflejo está dado por

$$(x, y) \longmapsto (x, -y - a_1x - a_3)$$

Hay fórmulas para $X(P_1+P_2)$ y $X(2P)$ también

• Ventajas de curvas en $\mathbb{F}_{2^k}$ (1) (computadoras son binarias) y

(2) si k fuera compuesto, hay cuerpos $\mathbb{F}_{2^l}$ entre $\mathbb{F}_{2^k}$ y $\mathbb{F}_2$ (esto hecho se puede aplicar para algunas cuentas) y

(3) Siguiendo una observación de Koblitz se puede ahorrar mucho los procedimientos de encriptar y desencriptar.

Def: Mapa de Frobenius:

$$\tau : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$$
$$\alpha \longmapsto \alpha^p$$

Prop: $\tau(\alpha\beta) = (\alpha\beta)^p = \alpha^p\beta^p = \tau(\alpha)\tau(\beta)$

$$\tau(\alpha+\beta) = (\alpha+\beta)^p = \sum_{i=0}^{p} \binom{p}{i} \alpha^i \beta^{p-i}$$

$$= \alpha^p + \beta^p \ (\text{mód } p)$$

$$= \tau(\alpha) + \tau(\beta)$$

τ es un homomorfismo de cuerpos

Ahora, sea $E \setminus \mathbb{F}_2$ y $P = (x,y)$ en $E(\mathbb{F}_{2^k})$. Para puntos $P \in E(\mathbb{F}_{2^k})$ definimos la acción de τ en P como

$$\tau(P) = (\tau(x), \tau(y)).$$

Prop: (1) $\tau(P) \in E(\mathbb{F}_{2^k})$

(2) $P, Q \in E(\mathbb{F}_{2^k}) \Rightarrow \tau(P+Q) \in E(\mathbb{F}_{2^k})$
$$\tau(P+Q) = \tau(P) + \tau(Q)$$

Dem (1): $P = (x,y) \in E(\mathbb{F}_{2^k}) \Rightarrow$

$$y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

$$\Rightarrow \tau(y)^2 + \tau(a_1)\tau(x)\tau(y) + \tau(a_3)\tau(y) - \tau(x)^3 - \tau(a_2)\tau(x)^2 - \tau(a_4)\tau(x) - \tau(a_6) = 0$$

Los $a_i \in \mathbb{F}_2$ y τ fija $\mathbb{F}_2$: $\tau(1) = 1^2$, $\tau(0) = 0$.

Entonces

$$r(y)^2 + a_1 r(x) r(y) + a_3 r(y) - r(x)^3 - a_2 r(x)^2 - a_4 r(x) - a_6 = 0$$

$$\Rightarrow (r(x), r(y)) \in E(\overline{\mathbb{F}}_{p^k}). \qquad \square$$

Algo parecido para (2).

Thm: $E \setminus \mathbb{F}_p$, $t = p+1 - \#E(\mathbb{F}_p)$. ($|t| \leq 2\sqrt{p}$)

(a) Sean α y β las raíces de $z^2 - tz + p$. Entonces

$$|\alpha| = |\beta| = \sqrt{p} \quad \text{y} \quad \forall k \geq 1$$

$$\#E(\mathbb{F}_{p^k}) = p^k + 1 - \alpha^k - \beta^k$$

(b) $\forall Q \in E(\overline{\mathbb{F}}_{p^k})$,

$$r^2(Q) - t\, r(Q) + pQ = 0$$

$$\uparrow$$

$$r(r(Q)).$$

La idea de Koblitz

nP: en vez de calcular nP con combinaciones de $2P$

~~hacer~~ se puede hacer con combinaciones de $r(P)$

Def. Una curva de Koblitz es una curva elíptica definida sobre $\mathbb{F}_2$ de la forma

$$E_a: \quad y^2 + xy = x^3 + a x^2 + 1$$

$$a \in \{0, 1\} \subset \mathbb{F}_2$$

- $\Delta_{E_a} = 1$

Obs. Recordamos nuestra notación ≈

$$E_0: \quad y^2 + xy = x^3 + 1$$

Obs. $\cdot E_0(\mathbb{F}_2) = \{(0,1), (1,1), (1,0), \mathcal{O}\}$

$$\Rightarrow \quad t = 2 + 1 - \#E_0(\mathbb{F}_2) = -1$$

Ahora para poder aplicar el teorema de antes consideramos el polinomio

$$\underbrace{z^2 + z + 2}_{-t}$$

Las raíces son $\alpha = \dfrac{-1+\sqrt{-7}}{2}$ $\quad \beta = \dfrac{-1-\sqrt{-7}}{2}$

Y, entonces, el final

$$\Rightarrow \quad \#E_0(\mathbb{F}_{2^k}) = 2^k + 1 - \left(\frac{-1+\sqrt{-7}}{2}\right)^k - \left(\frac{-1-\sqrt{-7}}{2}\right)^k$$

Pero también $\Rightarrow$ el mapa ~~$\tau^2 + \tau + 2$~~ τ verifica

$$\tau^2(P) + \tau(P) + 2P = \mathcal{O} \qquad \forall P \in E(\mathbb{F}_{2^k})$$

Ahora la idea es escribir $n \in \mathbb{Z}$ como una suma de potencias de τ: ¿Qué? τ no es un número sino una función!

Pero, $2 = -\tau - \tau^2$:

Ej. $\quad 7 = 1 + 3 \cdot 2 = 1 + 3(-\tau - \tau^2)$

$= 1 - 3\tau - 3\tau^2 = 1 - \tau - \tau^2 - 2\tau - 2\tau^2$

~~$1 - 3\tau - 3($~~ $= 1 - \tau - \tau^2 - \tau(-\tau - \tau^2) - \tau^2(-\tau - \tau^2)$

$= 1 - \tau + \tau^2 + \tau^3 + \tau^3 + \tau^4 - \tau^2$

$= 1 - \tau + 2\tau^3 + \tau^4 = 1 - \tau + (-\tau - \tau^2)\tau^3 + \tau^4$

$= 1 - \tau - \tau^5$