week 5 03.03.2022
for the Ravdvin. [uncertain]

More on the number of points.

Theorem 4.12.

Let E be an elliptic curve over $\mathbb{F}_q$ of order $q+1-t$.

Write $X^2-tX+q = (X-\alpha)(X-\beta)$ Then

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

for all $n \geq 1$.

How to compute $s_n = \alpha^n+\beta^n$?

$$\boxed{\begin{array}{l} \cdot\ s_0 = \alpha^0+\beta^0 = 1+1=2 \\ \cdot\ s_1 = t \\ \cdot\ s_n = s_{n-1}\cdot t - q\, s_{n-2}. \end{array}}$$

Proof: $s_0 = 1$, $s_1 = \alpha+\beta = t$ because $(X-\alpha)(X-\beta) = X^2 - \underbrace{(\alpha+\beta)}_{=t}X + \underbrace{\alpha\beta}_{=q}$

- $\alpha^2 - t\alpha + q = 0$ as α is a root of X^2-tX+q
- $\alpha^{n-2}\underbrace{(\alpha^2-t\alpha+q)}_{=0} = \alpha^n - \alpha^{n-1}t + \alpha^{n-2}q = 0 \quad (*_\alpha)$

Same for β:

- $\beta^2 - t\beta + q = 0$ as β is a root of X^2-tX+q
- $\beta^{n-2}\underbrace{(\beta^2-t\beta+q)}_{=0} = \beta^n - \beta^{n-1}t + \beta^{n-2}q = 0 \quad (*_\beta)$

$$(*_\alpha)+(*_\beta) = 0 = (\alpha^n+\beta^n) - (\alpha^{n-1}+\beta^{n-1})t + (\beta^{n-2}+\alpha^{n-2})q$$

$$\Leftrightarrow \alpha^n+\beta^n = (\alpha^{n-1}+\beta^{n-1})t - q(\alpha^{n-2}+\beta^{n-2})$$

$$s_n = s_{n-1}t - q\, s_{n-2}. \qquad \square.$$

APPLICATION: a quadratic twist always has order $q+1+t$, where $E: y^2=x^3+Ax+B$ has order $q+1-t$.

Proof: $s_0 = 2$

$s_1 = t$

$s_2 = t\cdot s_1 - q\cdot s_0 = t^2-2q$ $\qquad \#E(\mathbb{F}_{q^2}) = q^2+1-t^2+2q$

$$\#E(\mathbb{F}_{q^2}) = q^2+2q+1-t^2 = (q+1)^2-t^2 = \underbrace{(q+1-t)}_{=\#E(\mathbb{F}_q)}\underbrace{(q+1+t)}_{=\#E'(\mathbb{F}_q)}$$

Let E': $\delta y^2 = x^3+Ax+B$ where $\delta\in\mathbb{F}_q$ is a non-square; $\sqrt{\delta}\in\mathbb{F}_{q^2}$, $\sqrt{\delta}\notin\mathbb{F}_q$.

$\psi: E \to E'$ $\qquad$ ψ is an isomorphism not defined over $\mathbb{F}_q$ but

$(x,y)\mapsto(x,\sqrt{\delta}y)$ $\qquad$ defined over $\mathbb{F}_{q^2}$.