chapter 3.

- What are the points of order 2 on a curve $y^2 = x^3 + a_2 x^2 + a_4 x + a_6$?
- What are the points of order 3?

The points of order 2 are the $(x_0, 0)$ points, where x_0 are three distinct roots of $x^3 + a_2 x^2 + a_4 x + a_6$.

if x_0 is such a root, then translate it to 0: $(x - x_0)(x^2 + a'x + b')$

with $(x-x_0)\left((x-x_0)^2 + \underbrace{(a_2 + 3x_0)}_{a'}(x-x_0) + \underbrace{3x_0^2 + 2a_2 x_0 + a_4}_{b'}\right)$

The other points of order 2 are: $(x_1, 0)$ and $(x_2, 0)$ where x_1, x_2 are two distinct roots of $x^2 + a'x + b'$.

There are in K if $a'^2 - 4b'$ is a square.

The points of order 3 are inflexion points (flex points).

$(u(v(x))' = u'(v(x))v'$

$(\sqrt{x})' = \frac{1}{2\sqrt{x}}$

$y^2 = x^3 + ax + b$ (or $x^3 + a_2 x^2 + a_4 x + a_6$).

let's look at $f = \sqrt{x^3 + a_2 x^2 + a_4 x + a_6}$ roots of the 2nd derivative:

$$g(x) = f''(x) f - \tfrac{1}{2} f'^2 = \frac{1}{2}\left(3x^4 + 4a_2 x^3 + 6a_4 x^2 + 12a_6 x + (4a_2 a_6 - a_4^2)\right)$$

assume $4a_2 a_6 - a_4^2 = 0 \rightarrow (0, \sqrt{a_6})$ is a point of order 3.

the 8 points are $(x_0, \pm y_0)$ where x_0 is a root of $g(x)$, and (x_0, y_0) satisfies the equation.

the ninth point is $\mathcal{O}$.

2022.02.22.

Points of finite order: torsion points.

A point $P \in E(\bar{K})$ has (finite) order m if $mP = \mathcal{O}$.
Otherwise, P has infinite order (over a field $K = \mathbb{Q}$ or $\mathbb{C}$ for example).
If P has finite order, P is a **torsion point**, or **m-torsion point**.

Over a finite field $\mathbb{F}_q$, all points have finite order, $E(\mathbb{F}_q)$ is finite: each point is a torsion point.

notation: $E[m] = \{ P \in E(\bar{K}) : mP = \mathcal{O} \}$ $\bar{K}$ = algebraic closure of K it mean: can take any extension of K

$E[m]$ is the set of m-torsion points.

$E[2]$ is the group of points of order 2.
$E[4]$ is made of the points of order 4 and contains the points of order 2:
$E[2] \subset E[4]$ indeed, if $2P = \mathcal{O}$, then a fortiori $4P = \mathcal{O}$ and $P \in E[4]$.

tutorial: what are the points of order 2, order 3? (in characteristic not 2, not 3).
→ there are 4 points of order 2, and 9 points of order 3 counting with $\mathcal{O}$.

$E[n]$ contains always $\mathcal{O}$.

$y^2 = (x-r_0)(x-r_1)(x-r_2)$ with $r_i \in \bar{K}$

$E[2] = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. if $\text{char} \neq 2$ → $E[2] = \{ \mathcal{O}, (r_0,0), (r_1,0), (r_2,0) \}$

and the structure is such that $2(r_i,0) = \mathcal{O}$, $(r_i,0) + (r_j,0) = (r_k,0)$ for i,j,k all distincts.
→ **there are n^2 points of order n.** It will be proven later.

Theorem (3.2 p 79)

Let E be an elliptic curve over a field K and let n be a positive integer.
if $\text{char}(K) \nmid n$, or $\text{char}(K) = 0$, then

$$E[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

if $\text{char}(K) = p > 0$ and $p \mid n$, write $n = p^v n_0$ with $p \nmid n_0$. Then (v = valuation of n at p; p does not divide n_0)

$$E[n] \simeq \mathbb{Z}/n_0\mathbb{Z} + \mathbb{Z}/n_0\mathbb{Z} \quad \text{or} \quad E[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n_0\mathbb{Z}.$$

ordinary curve $E[p] \simeq \mathbb{Z}/p\mathbb{Z}$
supersingular curve $E[p] \simeq 0$. (only $\mathcal{O}$).
↳ meaning superspecial.

Supersingular curves where the first to be used in crypto because their order was known.
→ $E_1 : y^2 = x^3 - ax$ / $\mathbb{F}_p$ $p \equiv 3 \bmod 4$, has order $p+1$ and is supersingular.
→ $E_2 : y^2 = x^3 + b$ / $\mathbb{F}_p$, $p \equiv 2 \bmod 3$, has order $p+1$ and is supersingular.

- shows that $\# E_1 = p+1$.

Other curves: supersingular curves in char 2, char 3, with the help of the Cunningham project.

17. 02. 2022.

Morphisms: $\mathcal{E}_1 : y_1^2 = x_1^3 + a_1 x_1 + b_1$, $\mathcal{E}_2 : y_2^2 = x_2^3 + a_2 x_2 + b_2$

are two elliptic curves defined over a field K.

A morphism $\phi : \mathcal{E}_1 \longrightarrow \mathcal{E}_2$ is a mapping

$$\phi : (x_1, y_1) \longmapsto (\phi_x(x_1, y_1), \phi_y(x_1, y_1))$$

where ϕ_x and ϕ_y satisfy the equation of $\mathcal{E}_2$:

$$\phi_y^2 = (\phi_x)^3 + a_2 \phi_x + b_2$$

and ϕ_x, ϕ_y are in the function field of $\mathcal{E}_1$: $\overline{K}(\mathcal{E}_1)$

where $\overline{K}$ denotes the algebraic closure: it means for us that while $\mathcal{E}_1$ and $\mathcal{E}_2$ are defined over K, ϕ_x and ϕ_y can have coefficients in an extension of K.

K-morphisms, L-morphisms: morphisms ϕ with $\phi_x, \phi_y \in K(\mathcal{E}_1)$, resp. morphisms ϕ with $\phi_x, \phi_y \in L(\mathcal{E}_1)$ where L is an extension of K, for example $\mathbb{F}_{q^2}$ is an extension of $\mathbb{F}_q$, $\mathbb{Q}(i)$ is an extension of $\mathbb{Q}$ with $i^2 = -1$.

Homomorphisms: morphisms respecting the group law

Isomorphisms: invertible homomorphisms

Endomorphisms: homomorphisms from a curve to itself

Automorphisms: invertible endomorphisms.

There is also:

Epimorphism: surjective homomorphism, $\forall Q \in \mathcal{E}_2, \exists P \in \mathcal{E}_1, \phi(P) = Q$ i.e. there is always a preimage.

Monomorphism: injective homomorphism: $\phi(P_1) = \phi(P_2) \Rightarrow P_1 = P_2$ i.e. an injection maps distinct points to distinct images.

The **degree** of an K-morphism $\phi : \mathcal{E}_1 \longrightarrow \mathcal{E}_2$ can be expressed in terms of the degree of extension of the corresponding function fields:

$$\phi : (x_1, y_1) \in \mathcal{E}_1(K) \longmapsto (\phi_x(x_1, y_1), \phi_y(x_1, y_1)) \in \mathcal{E}_2(K)$$

induces an extension of function fields:

a function in $K(\mathcal{E}_2)$ is of the form $f(x_2, y_2)$, then we can express it in $K(\mathcal{E}_1)$ thanks to $(x_2, y_2) = (\phi_x(x_1, y_1), \phi_y(x_1, y_1))$: this becomes

$$f(\phi_x(x_1, y_1), \phi_y(x_1, y_1)) \in K(\mathcal{E}_1).$$

and deg ϕ = degree of the induced extension of fields:

$$\deg \phi = [K(\mathcal{E}_1) : K(\mathcal{E}_2)].$$

17.02.2022

Operations on morphisms:

- one can compose homomorphisms $\phi_1 : \mathcal{E}_1 \to \mathcal{E}_2$ and $\phi_2 : \mathcal{E}_2 \to \mathcal{E}_3$
- we can also add homomorphisms $\phi : \mathcal{E}_1 \longrightarrow \mathcal{E}_2$ and $\psi : \mathcal{E}_1 \longrightarrow \mathcal{E}_2$

$$(\phi +_1 \psi)(P) = \phi(P) +_2 \psi(P)$$

$+_1$: addition on $\mathcal{E}_1$ ↗ ↖ $+_2$: addition on $\mathcal{E}_2$

- Automorphisms of $\mathcal{E}$ form a group $\mathrm{Aut}(\mathcal{E})$ under composition $\circ$
- Homomorphisms $\mathcal{E}_1 \longrightarrow \mathcal{E}_2$ form a $\mathbb{Z}$-module $\mathrm{Hom}(\mathcal{E}_1, \mathcal{E}_2)$ under addition $+$
- Endomorphisms of $\mathcal{E}$ form a ring $\mathrm{End}(\mathcal{E})$ under addition and composition $(+, \circ)$

Over a finite field $\mathbb{F}_q$, we always have scalar multiplication $[m]_{m \in \mathbb{Z}}$ and Frobenius π_q,

$$\mathbb{Z}[\pi_q] \subseteq \mathrm{End}(\mathcal{E})$$

this is a ring, like
$\mathbb{Z}[i]$ or $\mathbb{Z}[\omega]$ are rings of integers of $\mathbb{Q}(i)$ and $\mathbb{Q}(\omega)$.

Theorem 3.2.

Let E be an elliptic curve $/K$ and let n a positive integer.
if $\mathrm{char}(K) \nmid n$, or $\mathrm{char}(K) = 0$, then

$$E[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

...

Let $n > 0$ $(n \in \mathbb{N})$, $\mathrm{char}(K) \nmid n$.
Choose a BASIS $(\vec{b_1}, \vec{b_2})$, that is two points (B_1, B_2) for $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$.
Any $P \in E[n]$ can be written in the form

$$P = m_1 B_1 + m_2 B_2 \quad \text{with } m_1, m_2 \text{ integers.}$$

m_1, m_2 are uniquely determined mod n.
Let $\alpha : E(\bar{K}) \to E(\bar{K})$ a ~~homomorphism~~.
Then α maps $E[n]$ into $E[n]$. There are $a, b, c, d \in \mathbb{Z}/n\mathbb{Z}$ s.t.

$$\alpha(B_1) = a B_1 + c B_2, \quad \alpha(B_2) = b B_1 + d B_2$$

and α is represented by a 2×2 matrix

$$\alpha_n = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

composing homomorphisms $\leftrightarrow$ multiplying their matrices.

Division polynomials.

$$[n]P = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x,y)}{\psi_n(x,y)^3} \right)$$

$\psi_0 = 0$
$\psi_1 = 1$
$\psi_2 = 2y$
$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$
$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$
$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3$ for $m \geq 2$
$\psi_{2m} = \frac{1}{2y}\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)$ for $m \geq 3$.
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad 4y\,\omega_m$

$\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}$
$\omega_m = \frac{1}{4y}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)$

corollary: $[n]$ has degree n^2.
$\to$ there are n^2 points of order 2
as $\#\mathrm{Ker}([n]) = n^2 = \deg([n])$

Legendre symbol. (4.3.2p 104) Is x a square modulo p?

$$\left(\frac{x}{p}\right) = \begin{cases} +1 & \text{if } x \text{ is a square: there exists } s \text{ such that } s^2 \equiv x \bmod p,\ s, x \neq 0 \bmod p \\ -1 & \text{if } x \text{ is not a square: } s^2 \equiv x \bmod p \text{ has no solution } s \\ 0 & \text{if } x \equiv 0 \bmod p. \end{cases}$$

It can be generalized to a finite field $\mathbb{F}_q$ where $q = p^n$ is a prime power:

$$\left(\frac{x}{\mathbb{F}_q}\right) = \begin{cases} +1 & \text{if } s^2 = x \text{ has a solution } s \in \mathbb{F}_q^* \ (s \text{ non-zero}) \\ -1 & \text{if } s^2 = x \text{ has no solution } s \in \mathbb{F}_q, \\ 0 & \text{if } x = 0 \end{cases}$$

Theorem 4.14. p105.

Let E be an elliptic curve defined by $y^2 = x^3 + Ax + B$ over $\mathbb{F}_q$. Then

$$\#E(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + Ax + B}{\mathbb{F}_q}\right)$$

PROOF. Let $x_0 \in \mathbb{F}_q$. If $x_0^3 + Ax_0 + B$ is a square and non-zero, there are two points $(x_0, \pm y_0)$ on $E(\mathbb{F}_q)$.

$$\to \sum_{\substack{x \in \mathbb{F}_q, \\ \left(\frac{x^3+Ax+B}{\mathbb{F}_q}\right) = 1}} 2 = \sum_{x \in \mathbb{F}_q, \left(\frac{x^3+Ax+B}{\mathbb{F}_q}\right) = 1} \underbrace{\underbrace{1 + \left(\frac{x^3+Ax+B}{\mathbb{F}_q}\right)}_{=1}}_{=2}$$

If $x_0^3 + Ax_0 + B$ is not a square, there isn't any point of x-coordinate x_0.

Because $\left(\frac{x^3+Ax+B}{\mathbb{F}_q}\right) = -1$ for a non-square x^3+Ax+B, we add 1 again to get 0 in the sum.

$$\sum_{x \in \mathbb{F}_q, \left(\frac{x^3+Ax+B}{\mathbb{F}_q}\right) = -1} 0 = \sum_{x \in \mathbb{F}_q, \left(\frac{x^3+Ax+B}{\mathbb{F}_q}\right) = 1} \underbrace{\underbrace{1 + \left(\frac{x^3+Ax+B}{\mathbb{F}_q}\right)}_{=-1}}_{=0}$$

Finally if $\left(\frac{x_0^3+Ax_0+B}{\mathbb{F}_q}\right) = 0$, there is one point of order 2 $(x_0, 0)$.

$$\sum_{x \in \mathbb{F}_q, \left(\frac{x^3+Ax+B}{\mathbb{F}_q}\right) = 0} 1 = \sum_{x \in \mathbb{F}_q, \left(\frac{x^3+Ax+B}{\mathbb{F}_q}\right) = 0} 1 + \left(\frac{x^3+Ax+B}{\mathbb{F}_q}\right)$$

Finally, in each case 1, -1 or 0 for the Legendre symbol, the formula is

$$\sum_{x \in \mathbb{F}_q} 1 + \left(\frac{x^3+Ax+B}{\mathbb{F}_q}\right) = q + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3+Ax+B}{\mathbb{F}_q}\right)$$

and we finish with the point at infinity:

$$\#E(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3+Ax+B}{\mathbb{F}_q}\right)$$

□

22. 02. 2022.

Intuition: $E : y^2 = x^3 + Ax + B$ over a field $\mathbb{F}_q$ is made of $\{ P(x,y) \in \mathbb{F}_q \times \mathbb{F}_q : y^2 = x^3 + Ax + B \} \cup \{\mathcal{O}\}$.
The set of coordinates (x,y) is $\mathbb{F}_q \times \mathbb{F}_q$, but the order of the curve is not of magnitude q^2, but q.

This is Hasse's theorem. (4.2 p97)

THEOREM (HASSE) Let E be an elliptic curve over a finite field $\mathbb{F}_q$. Then the order of $E(\mathbb{F}_q)$ satisfies

$$\left| q + 1 - \#E(\mathbb{F}_q) \right| \leq 2\sqrt{q}$$

THEOREM (WATERHOUSE 1969)
Let $q = p^n$ and let t such that $N = q + 1 - t$. There is an elliptic curve E defined over $\mathbb{F}_q$ such that $\#E(\mathbb{F}_q) = N$ iff $|t| \leq 2\sqrt{q}$ and t satisfies one of the following:

1) $\gcd(t, p) = 1$ ordinary curve

supersingular curves

2) n is even ($q = p^n$) and $t = \pm 2\sqrt{q}$
3) n is even, $p \not\equiv 1 \bmod 3$, and $t = \pm \sqrt{q}_{(n+1)/2}$ ← this is an integer if n is odd
4) n is odd, $p = 2$ or 3, and $t = \pm p$
5) n is even, $p \not\equiv 1 \bmod 4$, and $t = 0$
6) n is odd and $t = 0$.

Examples from Steven Galbraith (Book p. 185) § 9.10
Advances in Elliptic Curve Cryptography, LMS 317 p 199.

k	q	$\#E(\mathbb{F}_q)$	Group structure of $E(\mathbb{F}_{q^k})$
1	p^{2b}	$q \pm 2\sqrt{q} + 1$	$(\mathbb{Z}/(\sqrt{q} \pm 1)\mathbb{Z})^2$
2	cases (5), (6)	$q + 1$	$(\mathbb{Z}/(q+1)\mathbb{Z})^2$
3	case (3)	$q + \sqrt{q} + 1$	$(\mathbb{Z}/(q^{3/2} - 1)\mathbb{Z})^2$
3	case (3)	$q - \sqrt{q} + 1$	$(\mathbb{Z}/(q^{3/2} + 1)\mathbb{Z})^2$
4	2^{2b+1}	$q \pm \sqrt{2q} + 1$	$(\mathbb{Z}/(q^2+1)\mathbb{Z})^2$
6	3^{2b+1}	$q \pm \sqrt{3q} + 1$	$(\mathbb{Z}/(q^3+1)\mathbb{Z})^2$

k is the embedding degree w.r.t. a Tate or Weil pairing

22.02.2022.

Steven Galbraith's chapter 9 p 204, LMS 317. Table of supersingular curves.

$k=2$. $E: y^2 = x^3 + b$ over $\mathbb{F}_p$, $p \equiv 2 \bmod 3$.
$\#E(\mathbb{F}_p) = p+1$. Distortion map: $(x,y) \mapsto (\omega x, y)$ where $\omega^3 = 1$, $\omega \in \mathbb{F}_{p^2}$.

$k=2$. $E: y^2 = x^3 + ax$ over $\mathbb{F}_p$, $p \equiv 3 \bmod 4$.
$\#E(\mathbb{F}_p) = p+1$ Distortion map $(x,y) \longmapsto (-x, iy)$ where $i^2 = -1$, $i \in \mathbb{F}_{p^2}$.

$k=3$. $E: y^2 = x^3 + b$ over $\mathbb{F}_{p^2}$, $p \equiv 5 \bmod 6$, $b \in \mathbb{F}_{p^2}$, $b \notin \mathbb{F}_p$ is a square but not a cube.
$\#E(\mathbb{F}_p) = p^2 - p + 1$. Distortion map $(x,y) \mapsto \left(x^p / (\sqrt[3]{b}\, b^{\frac{p-2}{3}}),\ y^p / b^{\frac{p-1}{2}} \right)$, $\sqrt[3]{b} \in \mathbb{F}_{p^6}$.

$k=4$. $E_i: y^2 + y = x^3 + x + a_i$ over $\mathbb{F}_2$, where $a_1 = 0$ or $a_2 = 1$.
$\#E_i(\mathbb{F}_{2^l}) = 2^l \pm 2^{(l+1)/2} + 1$ (l odd)
Distortion map $(x,y) \mapsto (u^2 x + s^2,\ y + u^2 s x + s)$, where $u \in \mathbb{F}_{2^2}$ and $s \in \mathbb{F}_{2^4}$ satisfy
$u^2 + u + 1 = 0$ and $s^2 + (u+1)s + 1 = 0$.

$k=6$. $E_i: y^2 = x^3 - x + a_i$ over $\mathbb{F}_3$, where $a_1 = 1$ and $a_2 = -1$.
$\#E_i(\mathbb{F}_{3^l}) = 3^l \pm 3^{(l+1)/2} + 1$ (l odd)
Distortion map $(x,y) \mapsto (\alpha - x, iy)$ where $i \in \mathbb{F}_{3^2}$ and $\alpha \in \mathbb{F}_{3^3}$ satisfy
$i^2 = -1$ and $\alpha^3 - \alpha - a_i = 0$.

Examples of supersingular curves in characteristic 2 and 3.

Boneh, Lynn, Shacham, 2001, Short signatures from the Weil pairing. Table 1.

E_{-1}	$l = 79$	$= 7 \bmod 12$
E_{+1}	$l = 97$	$= 1 \bmod 12$
E_{+1}	$l = 149$	$= 5 \bmod 12$
E_{+1}	$l = 163$	$= 7 \bmod 12$
E_{-1}	$l = 163$	$= 7 \bmod 12$
E_{+1}	$l = 167$	$= 11 = -1 \bmod 12$

Lemma 1. The curve $E_{+1}: y^2 = x^3 + 2x + 1$ over $\mathbb{F}_{3^l}$ has $\#E_{+1}(\mathbb{F}_{3^l}) = \begin{cases} 3^l + 1 + 3^{\frac{l+1}{2}} & \text{if } l = \pm 1 \bmod 12 \\ 3^l + 1 - 3^{\frac{l+1}{2}} & \text{if } l = \pm 5 \bmod 12 \end{cases}$

The curve $E_{-1}: y^2 = x^3 + 2x - 1$ over $\mathbb{F}_{3^l}$ has $\#E_{-1}(\mathbb{F}_{3^l}) = \begin{cases} 3^l + 1 - 3^{\frac{l+1}{2}} & \text{when } l = \pm 1 \bmod 12 \\ 3^l + 1 + 3^{\frac{l+1}{2}} & \text{when } l = \pm 5 \bmod 12 \end{cases}$

→ Finds l such that $3^l + 1 + 3^{(l+1)/2}$, resp. $3^l + 1 - 3^{(l+1)/2}$ has a large prime factor.

$$\left(3^l + 1 + 3^{(l+1)/2}\right)\left(3^l + 1 - 3^{(l+1)/2}\right) = 3^{2l} + 2 \cdot 3^l + 1 - 3^{l+1} = 3^{2l} - 3^l + 1 = \Phi_6(3^l)$$

→ Cunningham project. $\Phi_6(3x^2) = 9x^4 - 3x^2 + 1 = (3x^2 - 3x + 1)(3x^2 + 3x + 1)$, $3x^2 = 3^l = 3^{1+2}$

$$3^{6l} - 1 = \left(3^{3l} - 1\right)\left(3^{3l} + 1\right) = \left(3^l - 1\right)\left(1 + 3^l + 3^{2l}\right)\left(3^{3l} + 1\right)$$

$$(3x^2)^3 + 1 = (3x^2 + 1)(9x^4 - 3x^2 + 1)$$

$$x^3 + 1 = (x+1)(x^2 - x + 1)$$

Aurifeuillean factorization

$\Phi_k(ax^2)$ factors if
- $a \equiv 1 \bmod 4$ and $a \equiv k \bmod 2a$, or
- $a \equiv 2, 3 \bmod 4$ and $2a \equiv k \bmod 4a$.

$E / \mathbb{F}_{3^\ell}$, ℓ odd, $\ell = 2m+1$. $\Phi_6(3x^2) = (3x^2+3x+1)(3x^2-3x+1)$

$\Phi_6(3^\ell) = \Phi_6(3^{2m+1}) = \Phi_6(3 \cdot 3^{2m}) = (3^{2m+1}+3^{m+1}+1)(3^{2m+1}-3^{m+1}+1)$

$\#E(\mathbb{F}_{3^\ell}) = 3^\ell - 3^{(\ell+1)/2} + 1 = 3^{2m+1} - 3^{m+1} + 1$.

$\Phi_6(3^{2m+1}) \mid 3^{3(2m+1)} + 1$. look for factors of $3^{3(2m+1)}+1 = 3^{3\ell}+1$.

$\Phi_6(x) \mid x^3 + 1$

$2 \cdot m + 1 = 97$: $3^{97} + 1$.