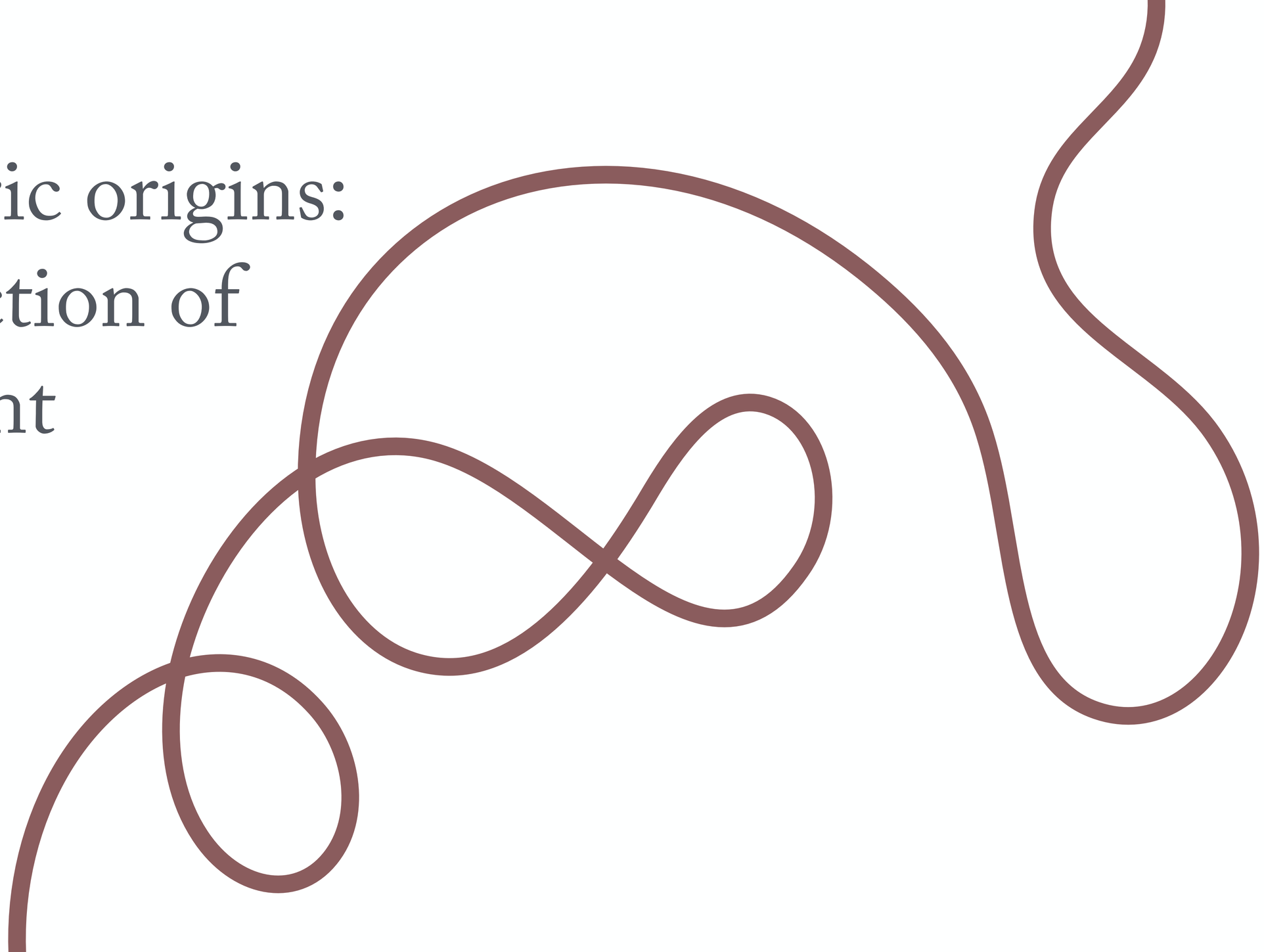
Visualizing Elliptic Curves over Finite Fields

Steve Trettel

Joint work with Nadir Hajouji

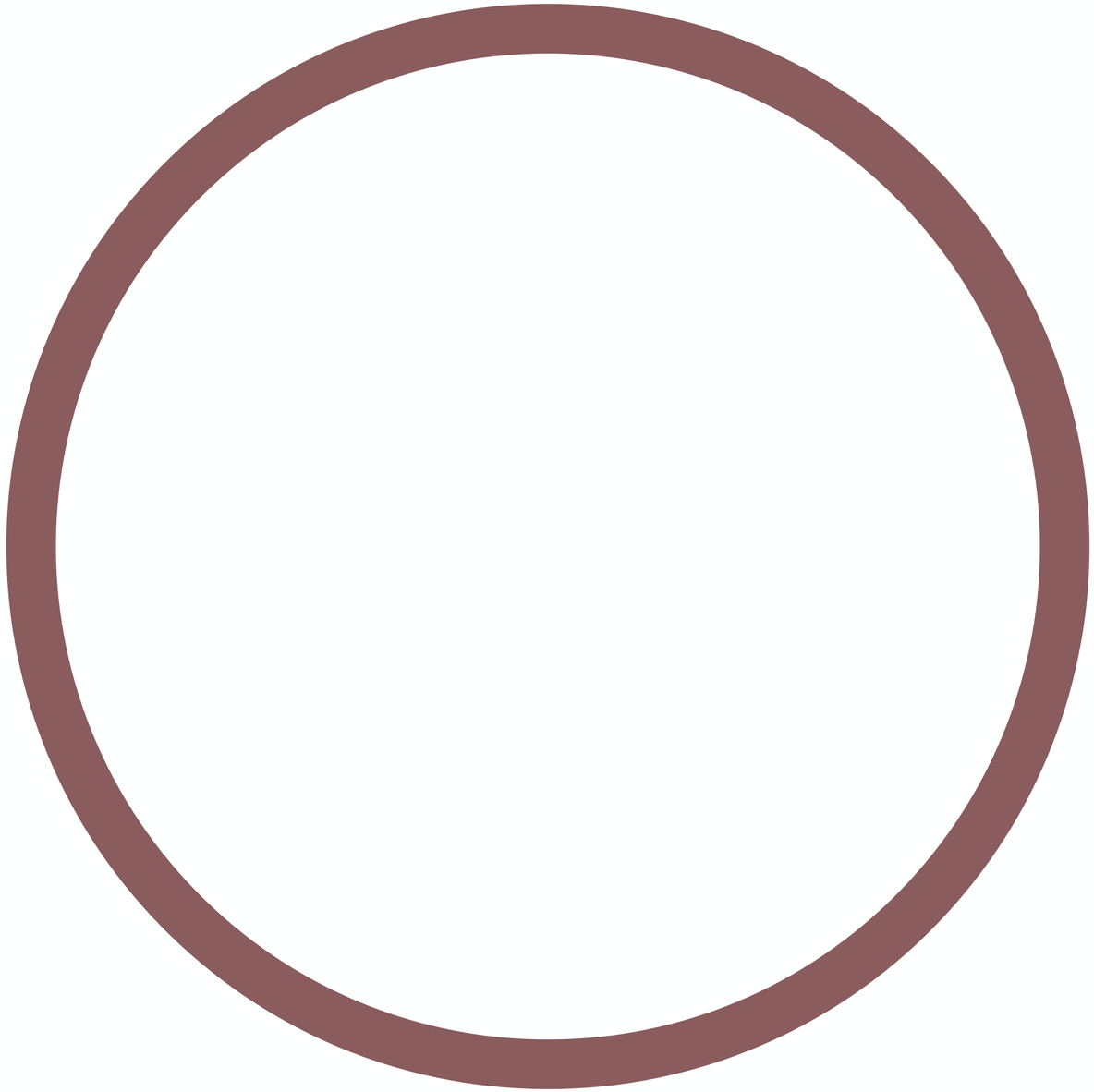
What is a curve?

Geometric origins: one direction of movement



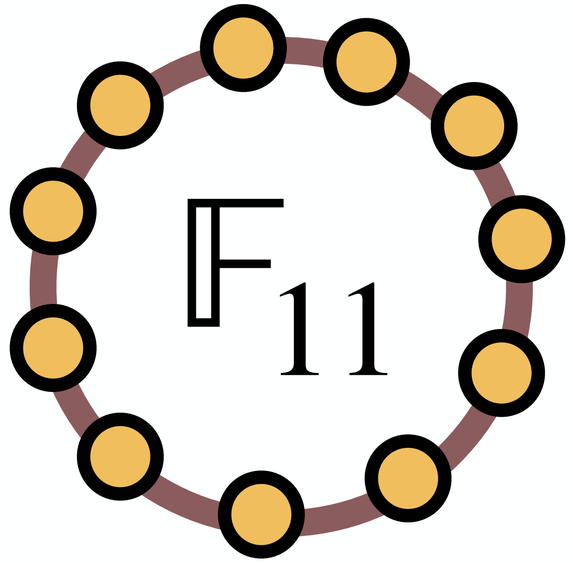
Algebraic recasting: one more variable than constraint

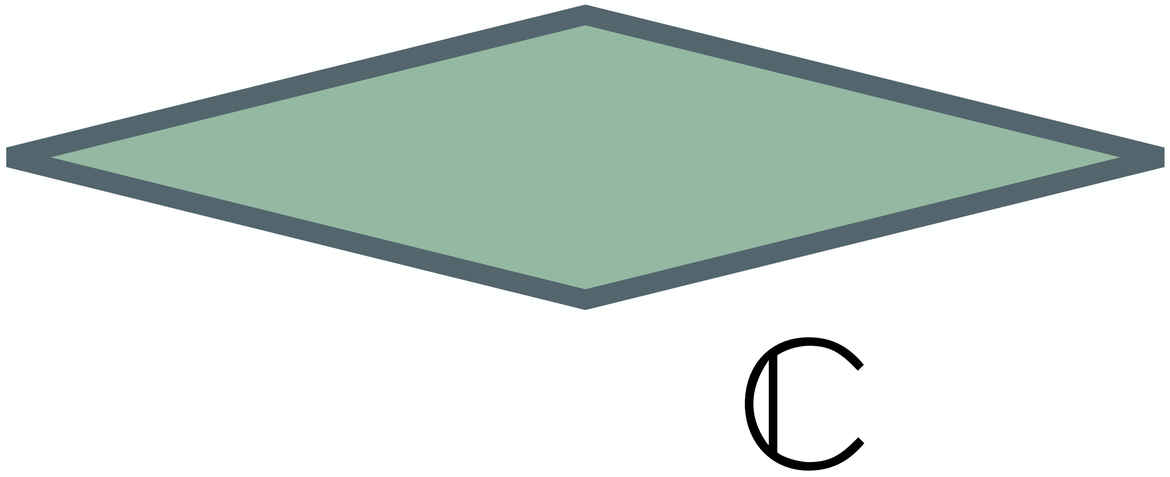
$$x^2 + y^2 = 1$$



Broadening our horizons:

These variables could come from many number systems





$$y = x^2$$

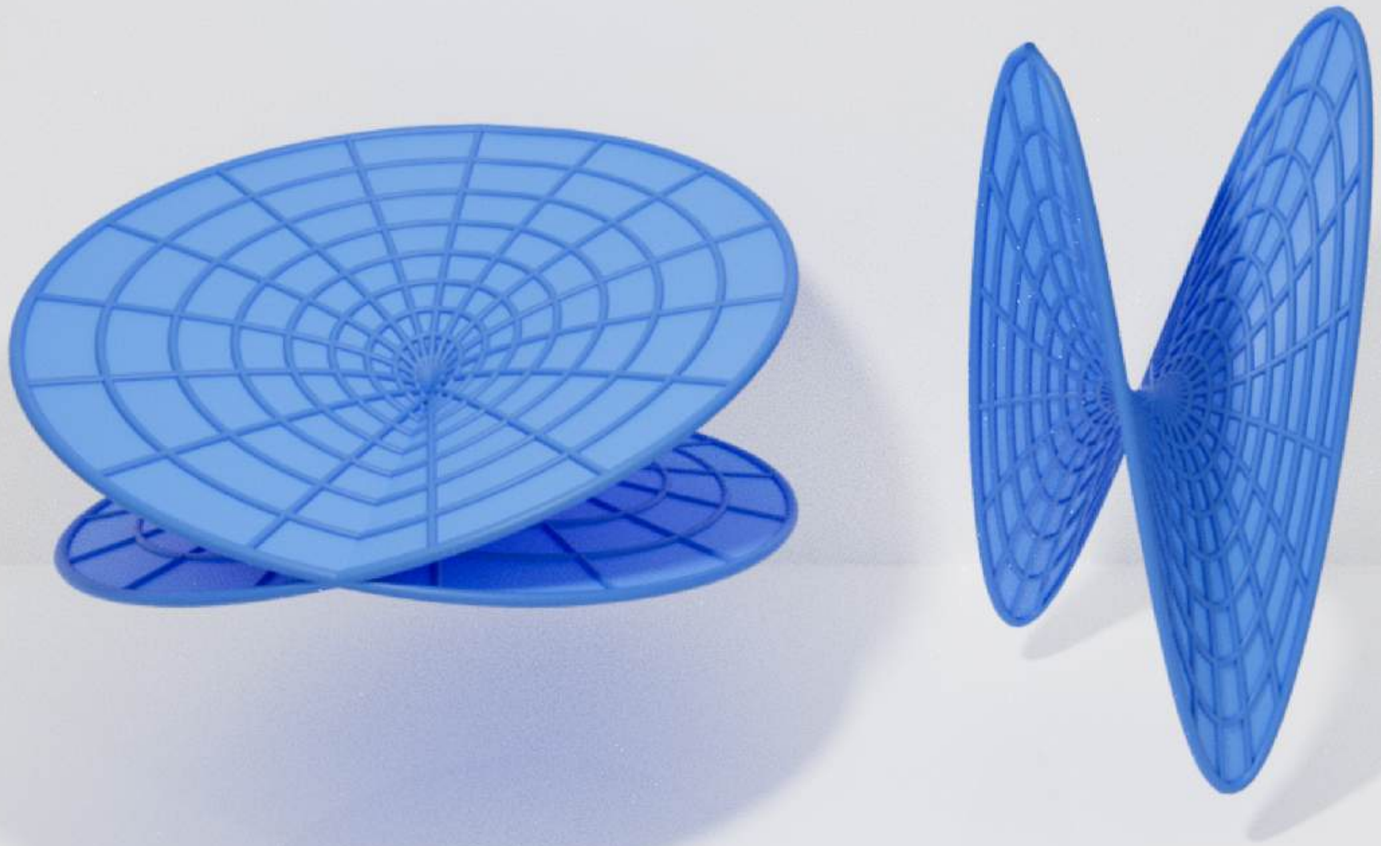
over

$$\mathbb{R}$$

$$y = x^2$$

over

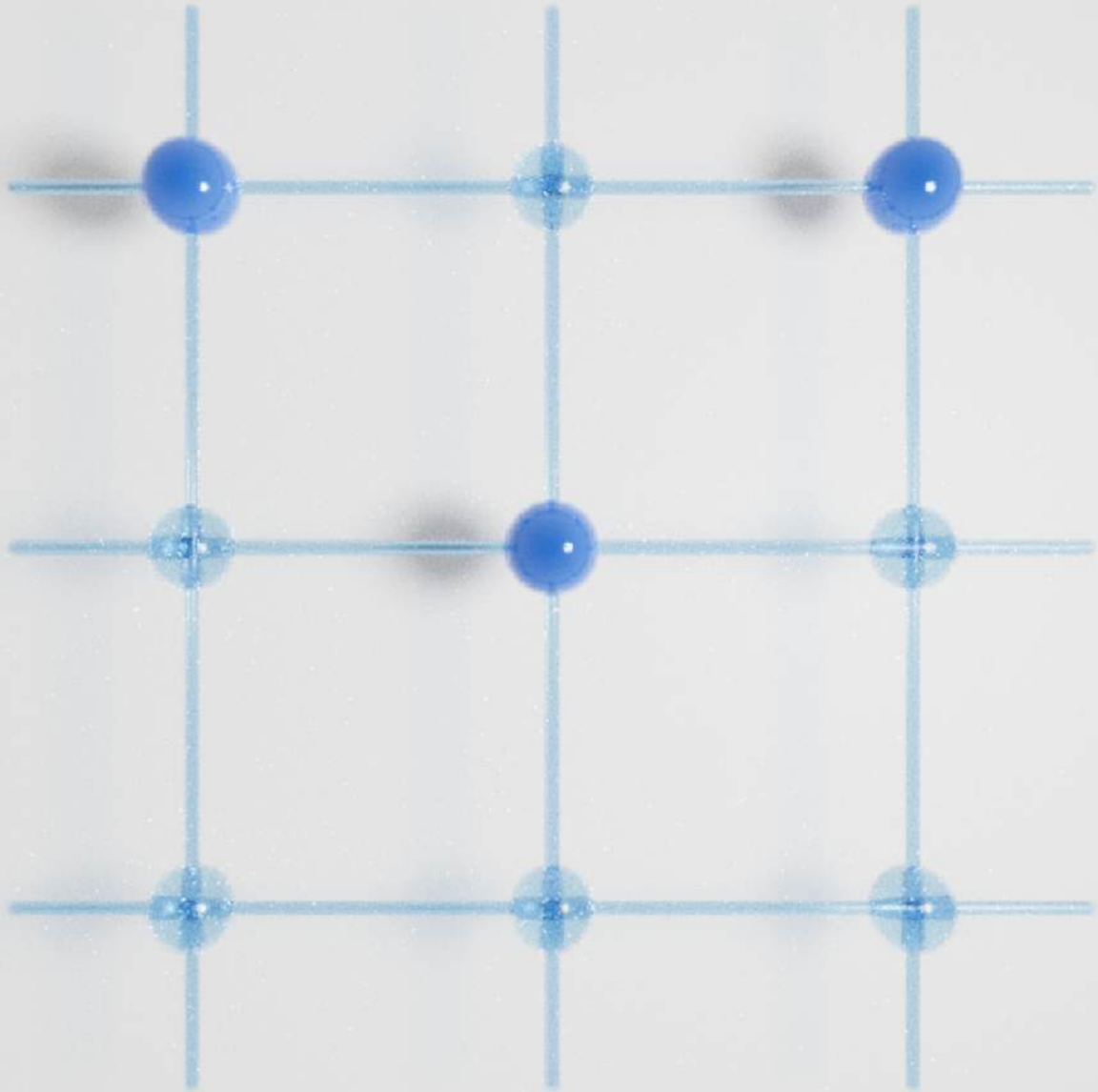
$$\mathbb{C}$$



$$y = x^2$$

over

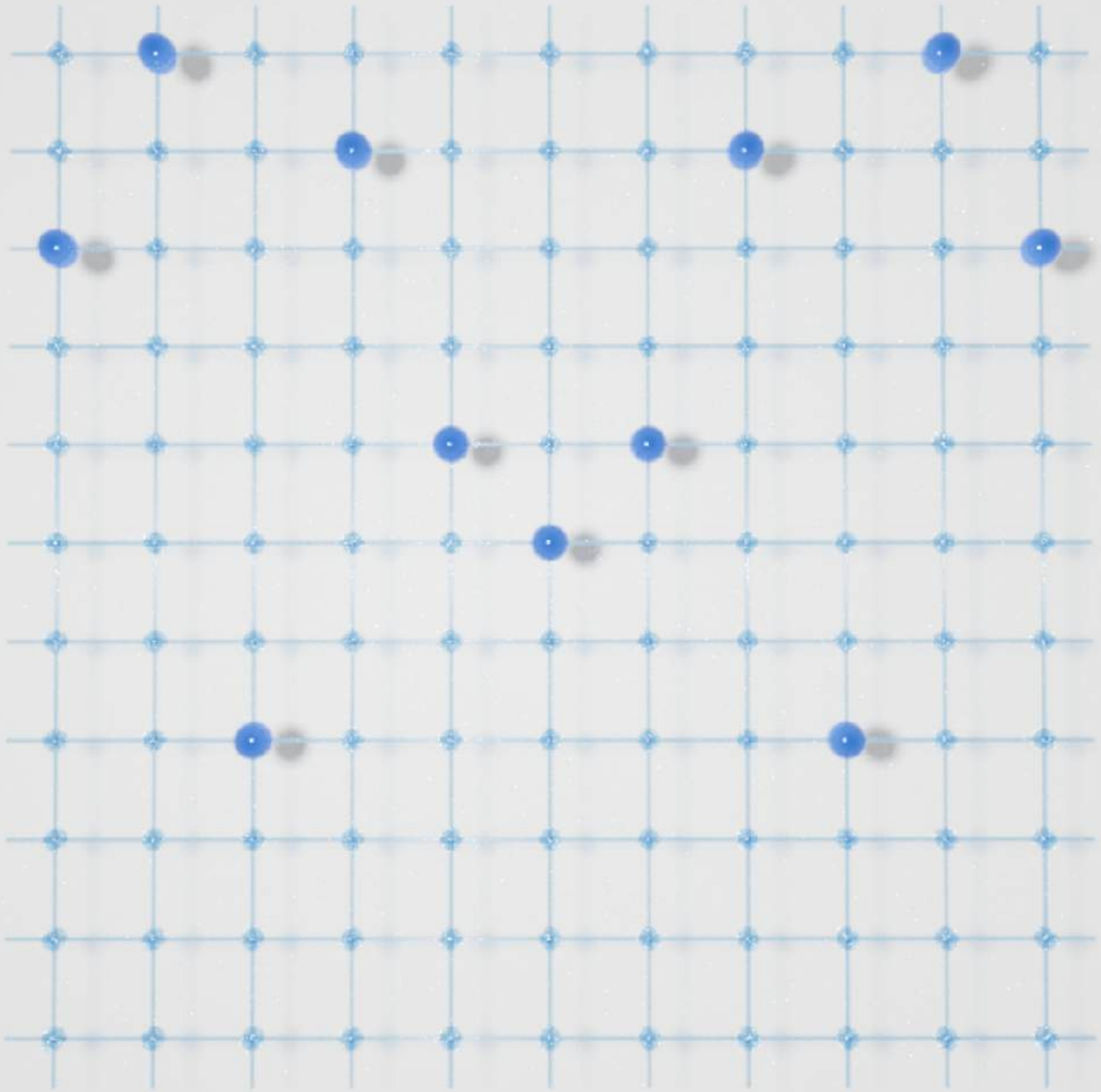
$$\mathbb{Z}/3\mathbb{Z}$$



$$y = x^2$$

over

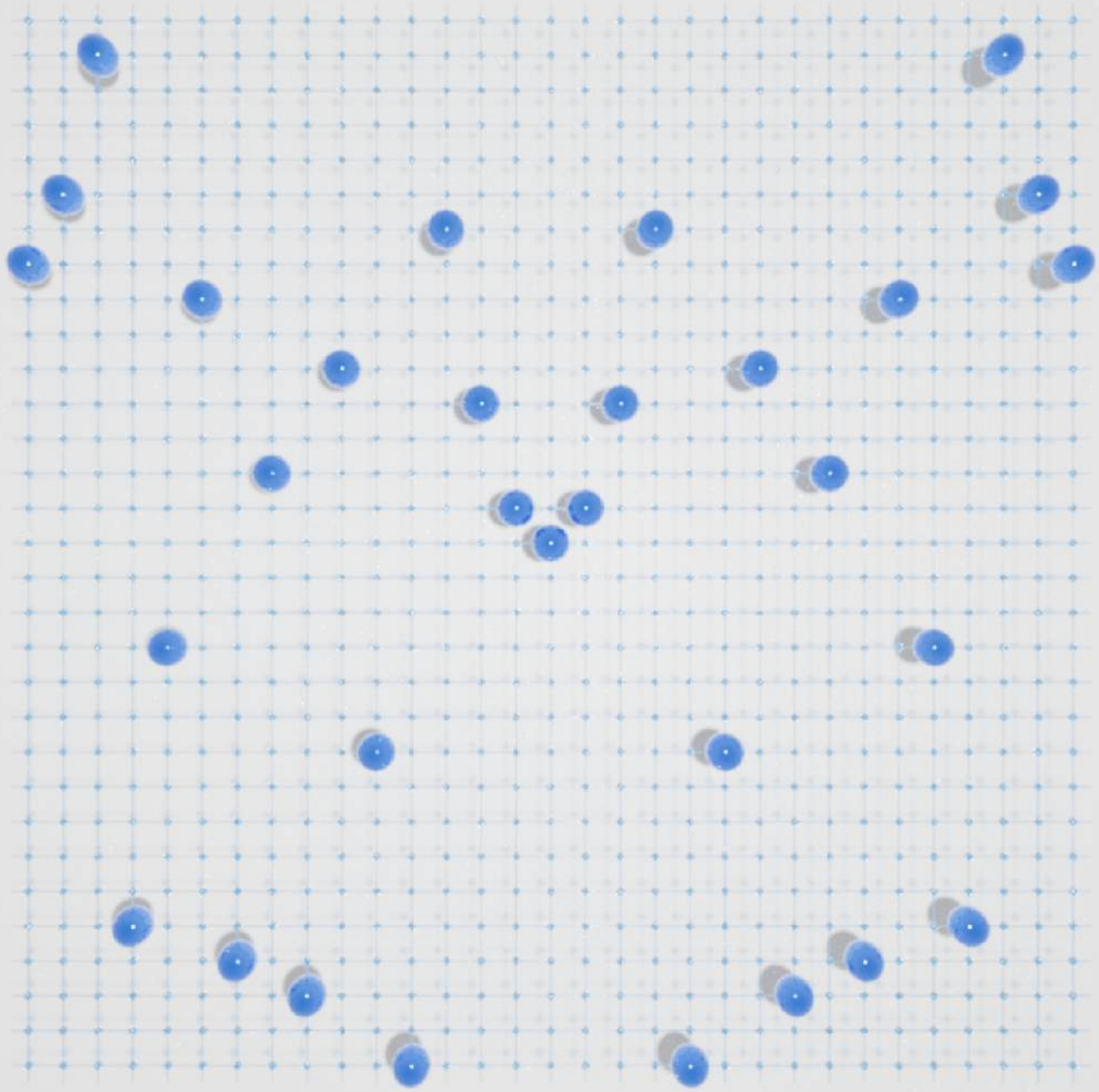
$$\mathbb{Z}/11\mathbb{Z}$$



$$y = x^2$$

over

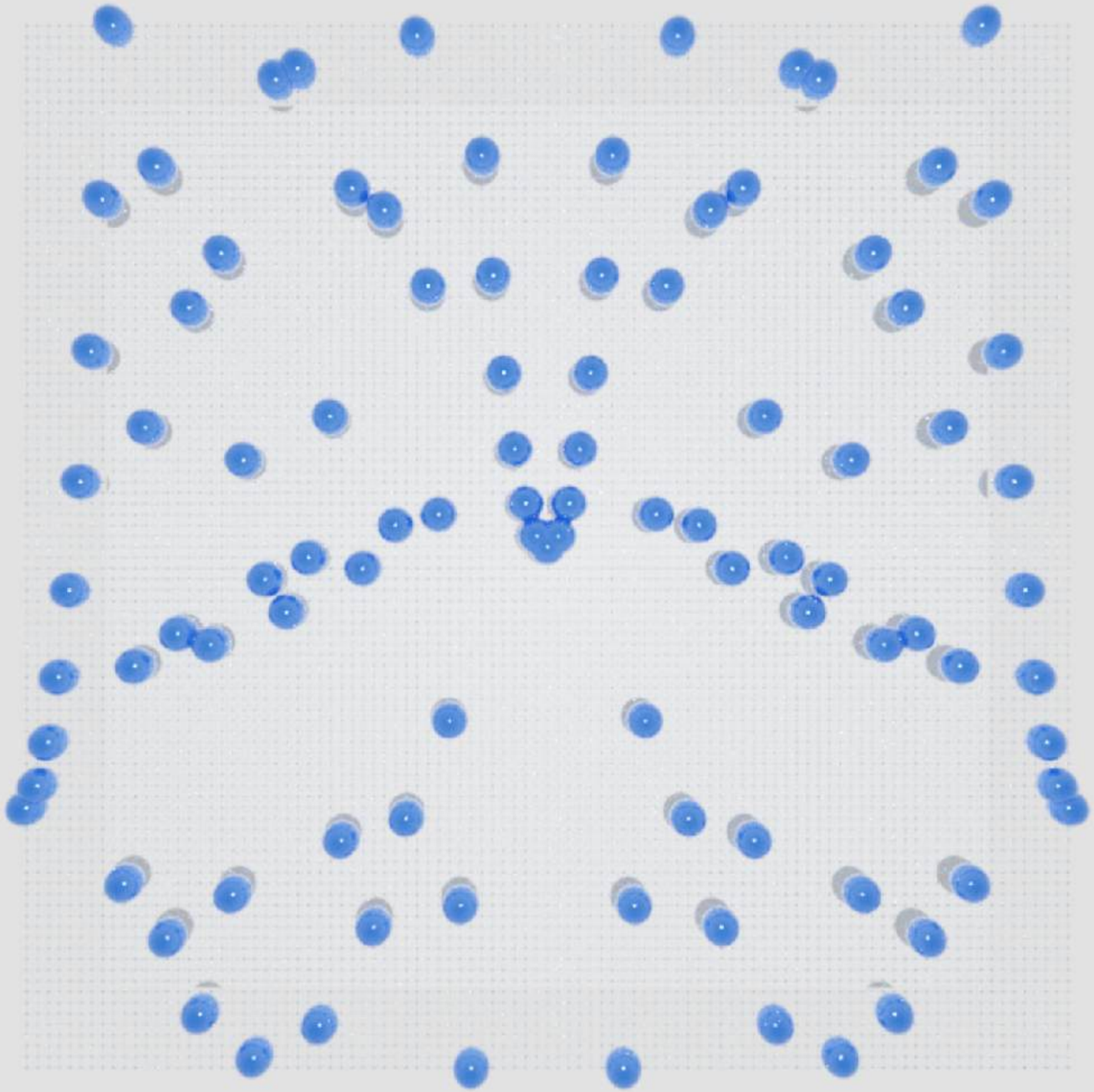
$$\mathbb{Z}/31\mathbb{Z}$$



$$y = x^2$$

over

$$\mathbb{Z}/97\mathbb{Z}$$

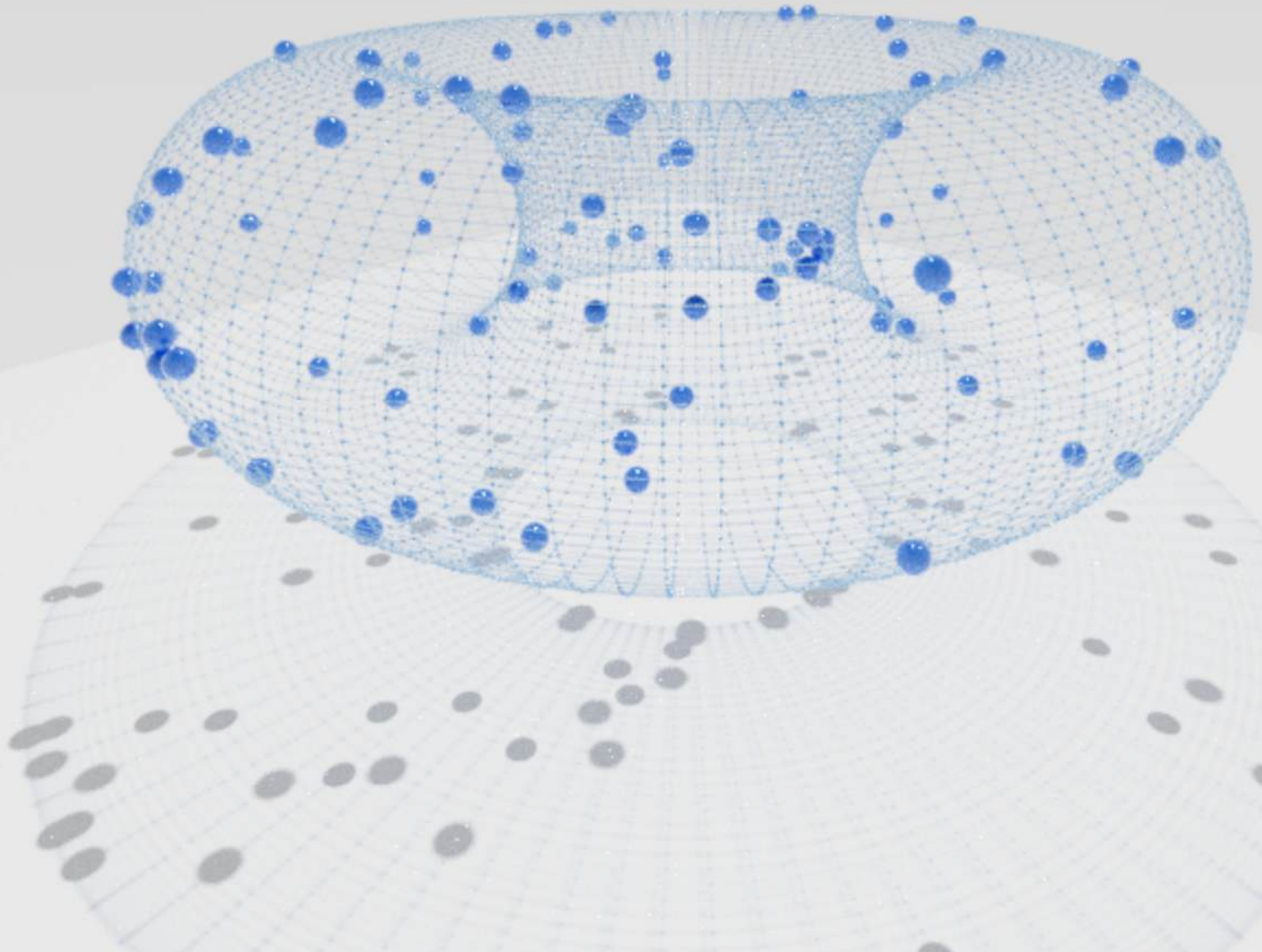


$$y = x^2$$

over

$$\mathbb{Z}/97\mathbb{Z}$$

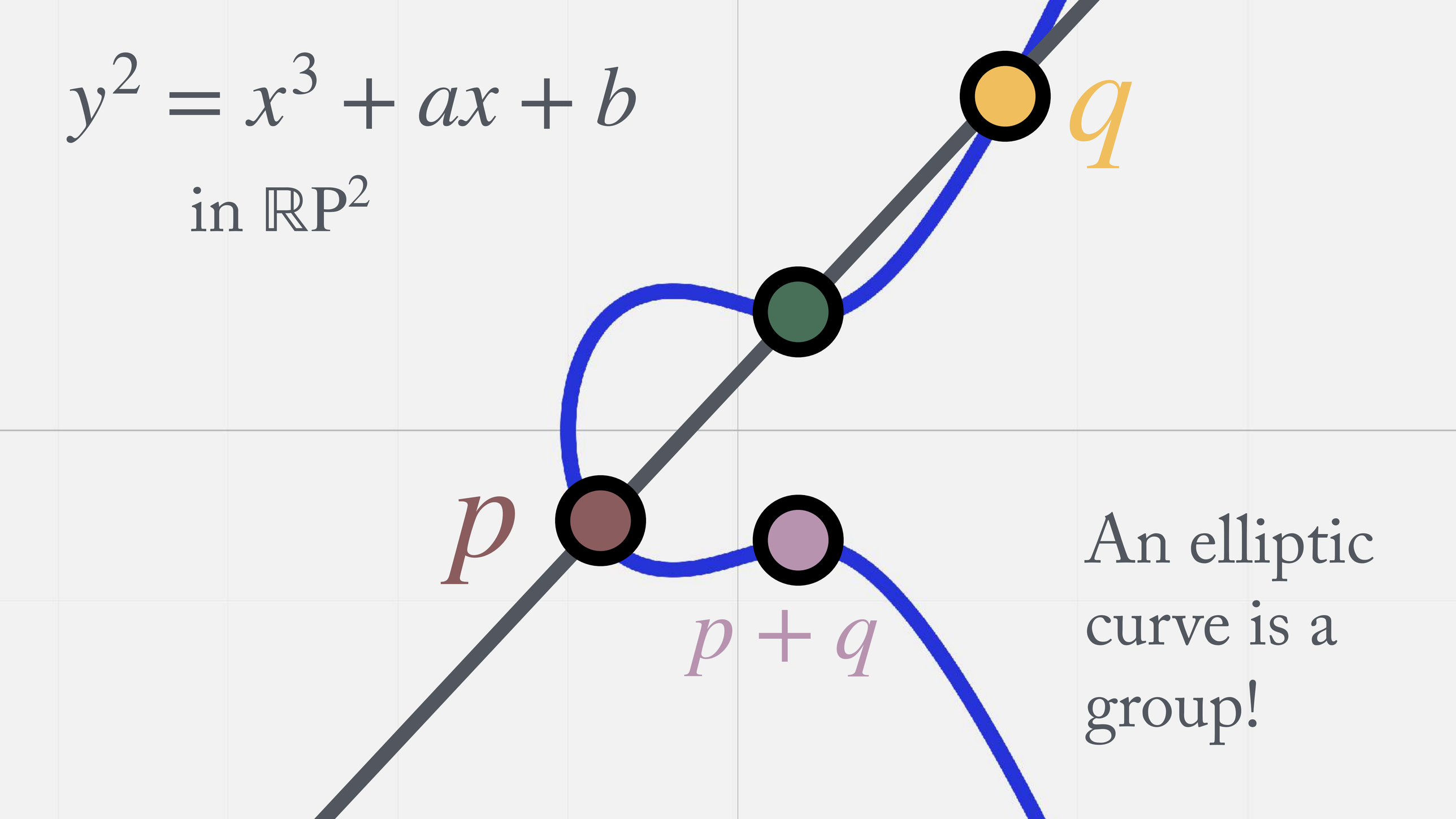
(rolled up)



II What is an elliptic curve?

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

in $\mathbb{R}\mathrm{P}^2$

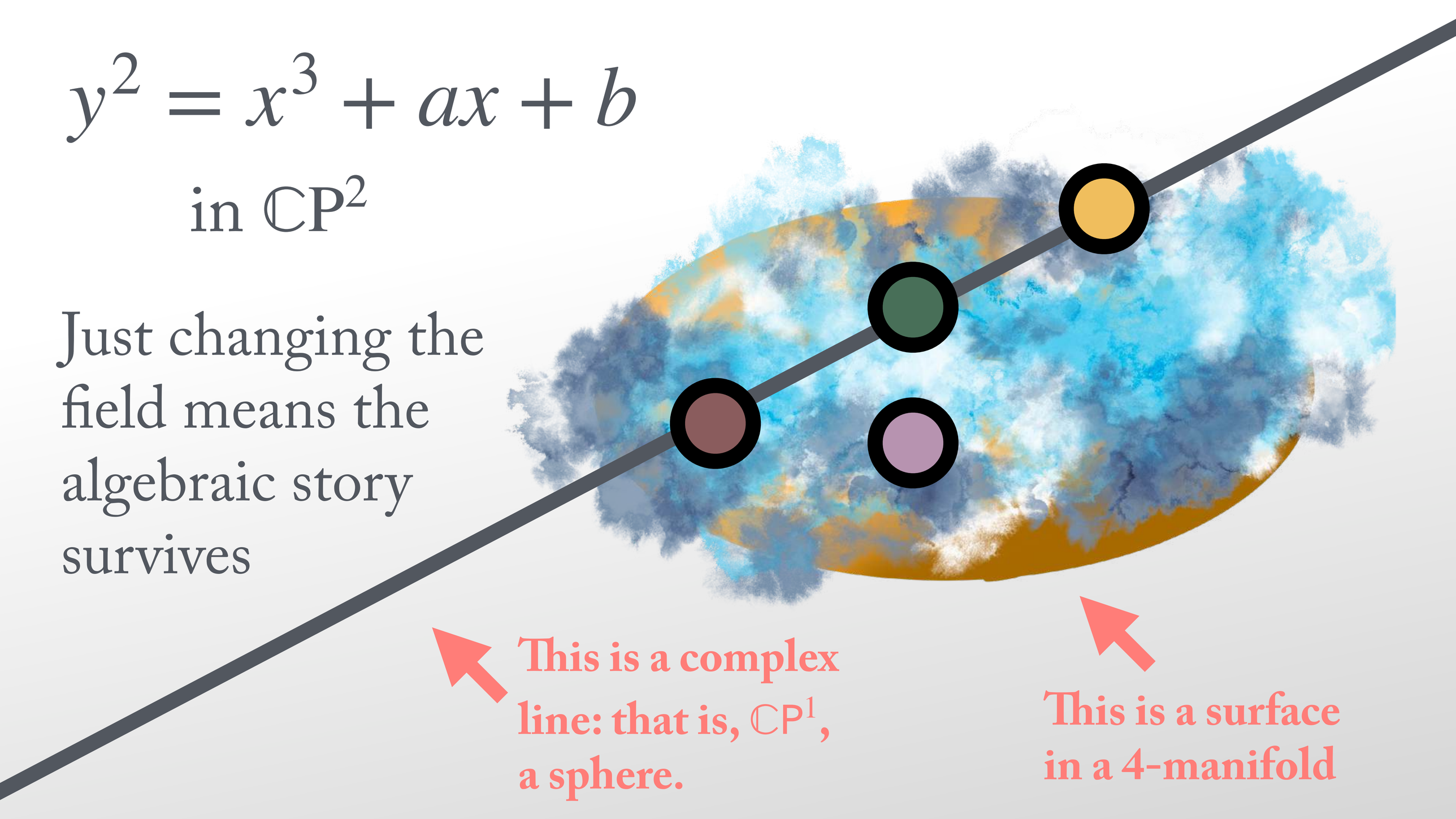


An elliptic curve is a group!

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

in $\mathbb{C}P^2$

Just changing the field means the algebraic story survives

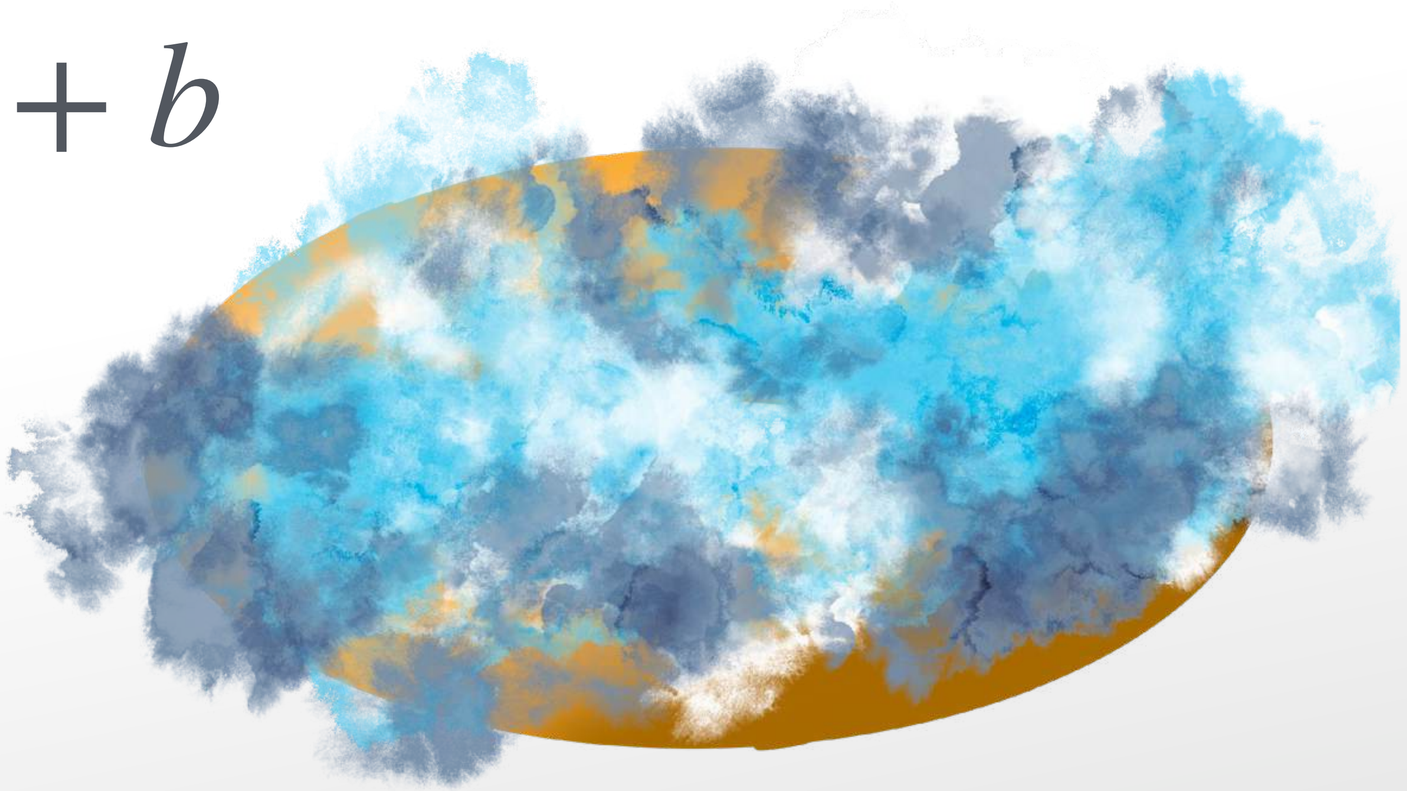


This is a complex line: that is, $\mathbb{C}P^1$, a sphere.

This is a surface in a 4-manifold

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

in $\mathbb{C}P^2$

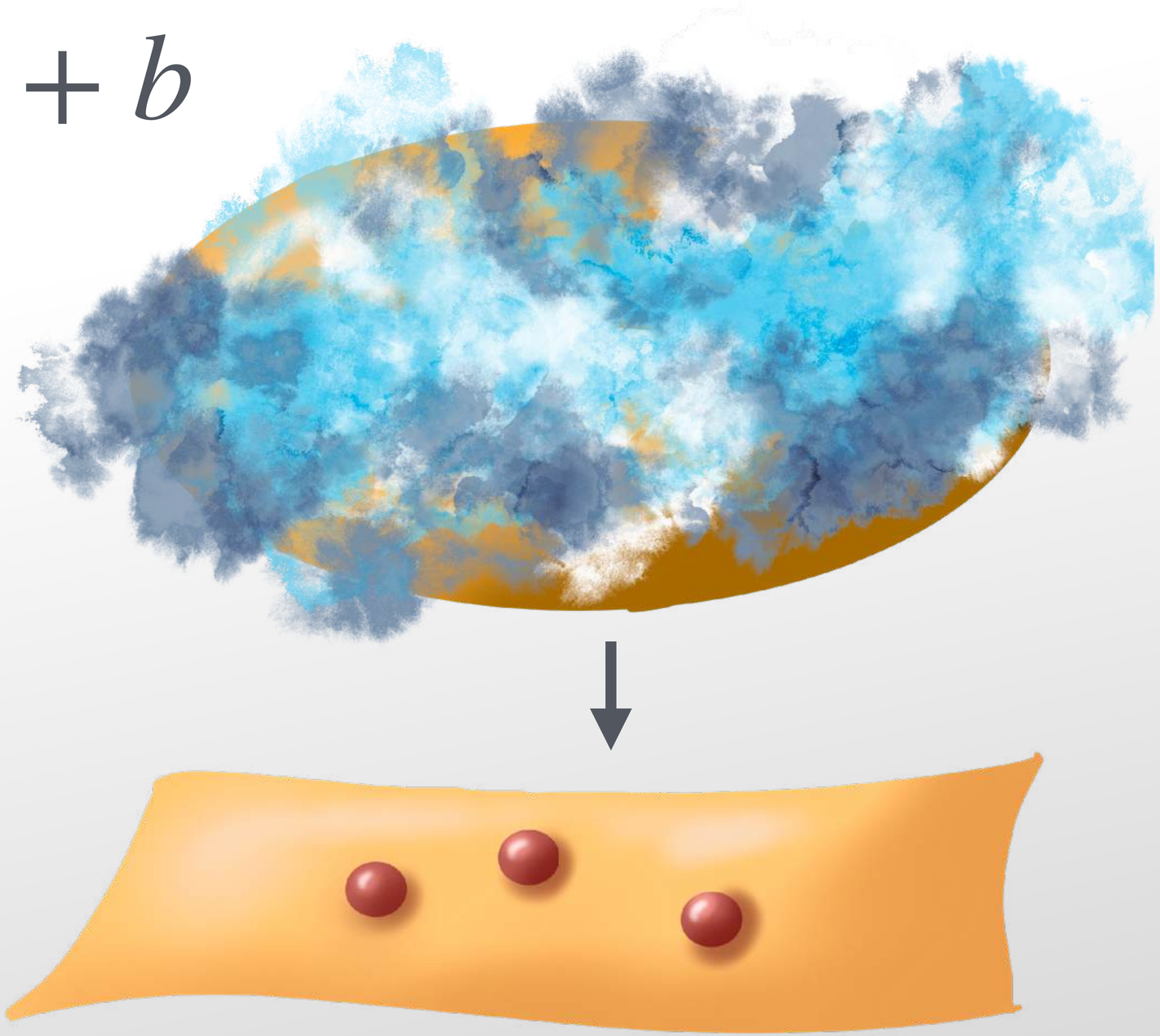


What does it look like over $\mathbb{C}$?

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

in $\mathbb{C}P^2$

(x, y)



x

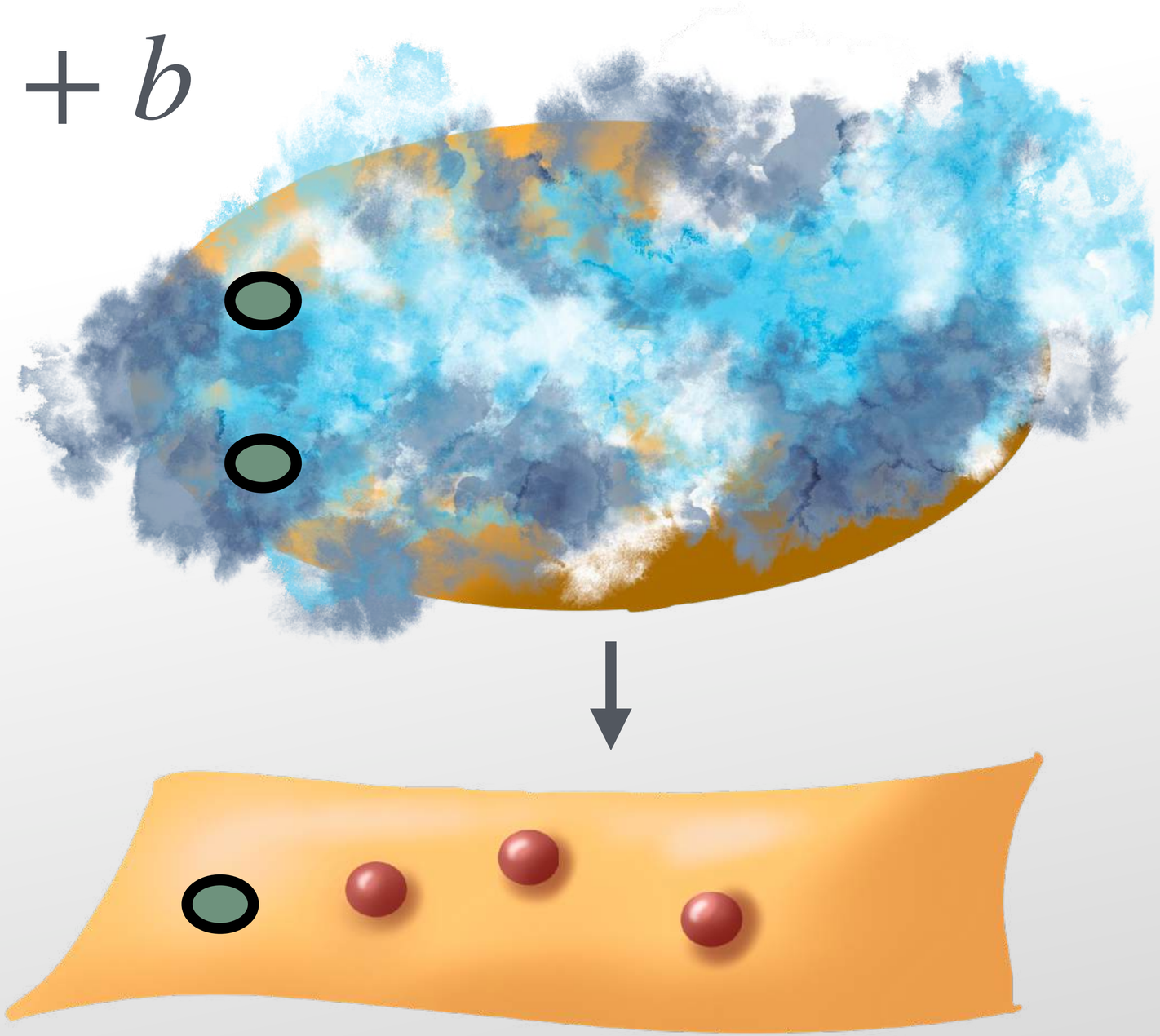
$$y^2 = x^3 + ax + b$$

in $\mathbb{C}P^2$

(x, y)

$\downarrow$

x



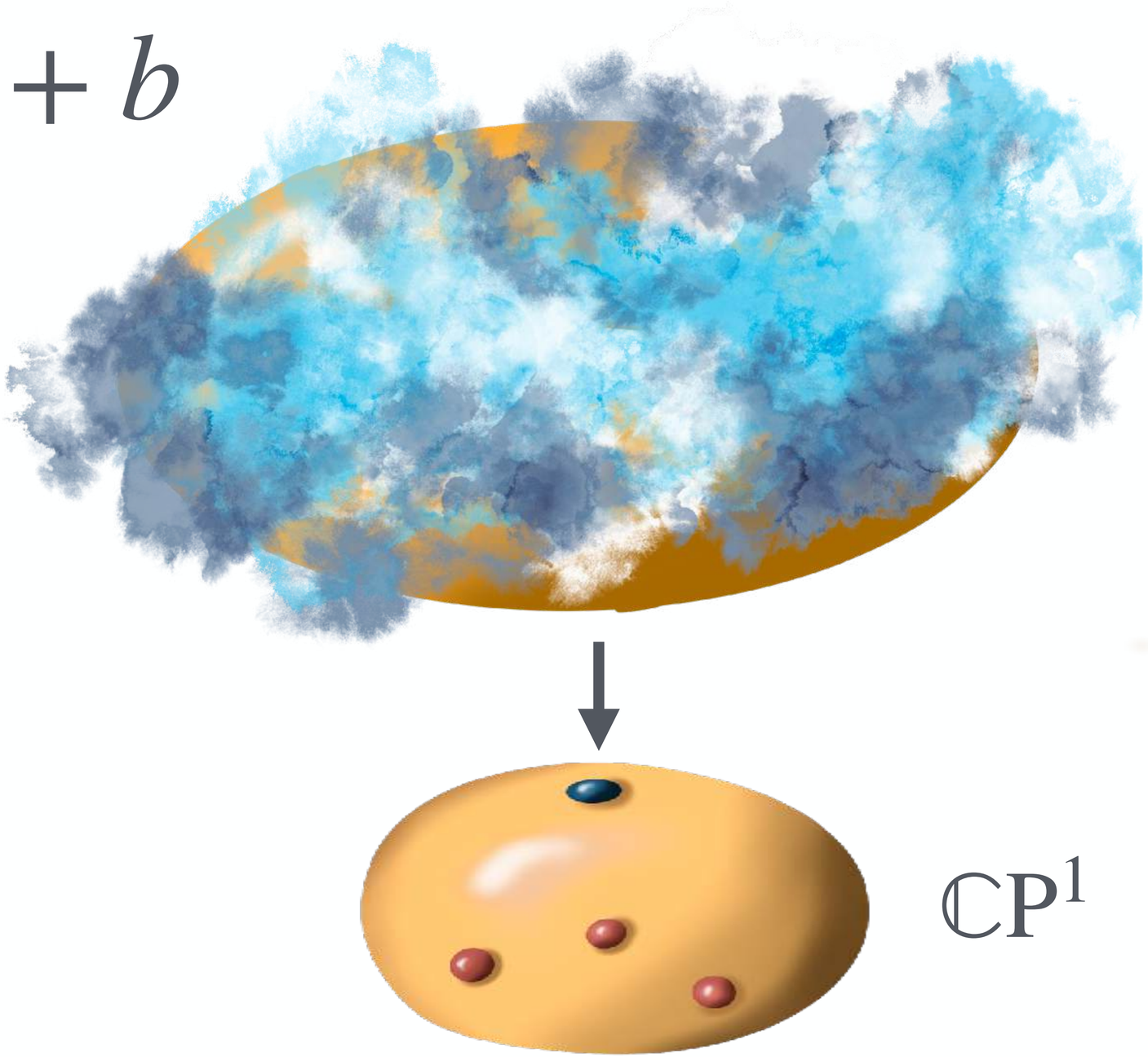
$$y^2 = x^3 + ax + b$$

in $\mathbb{C}\mathrm{P}^2$

(x, y)

$\downarrow$

x

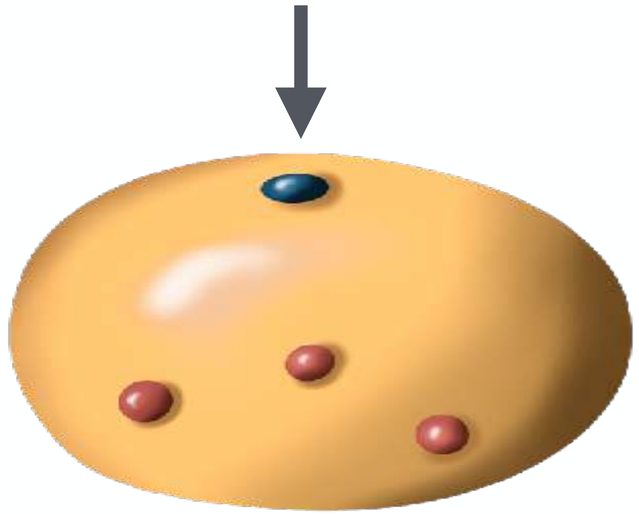


$\mathbb{C}\mathrm{P}^1$

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

in $\mathbb{C}\mathrm{P}^2$

(x, y)



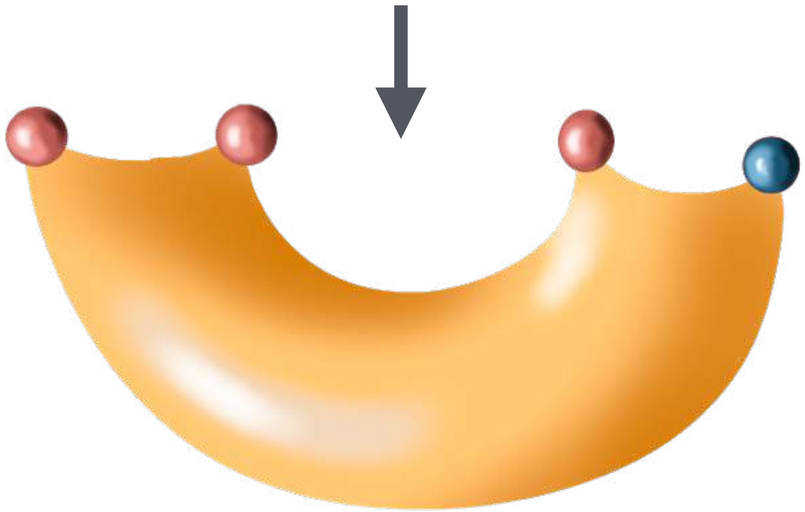
$\mathbb{C}\mathrm{P}^1$

x

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

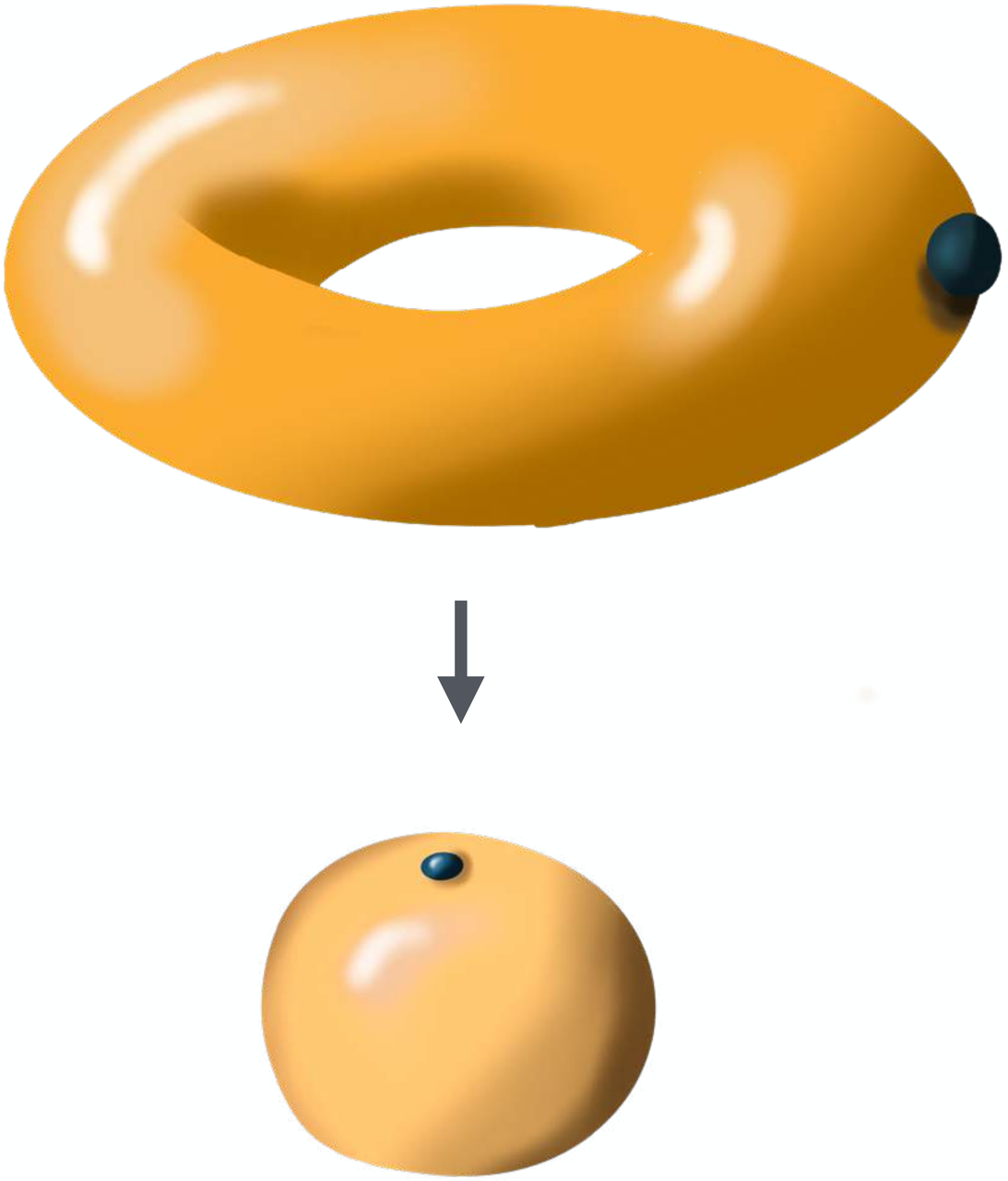
in $\mathbb{C}\mathrm{P}^2$

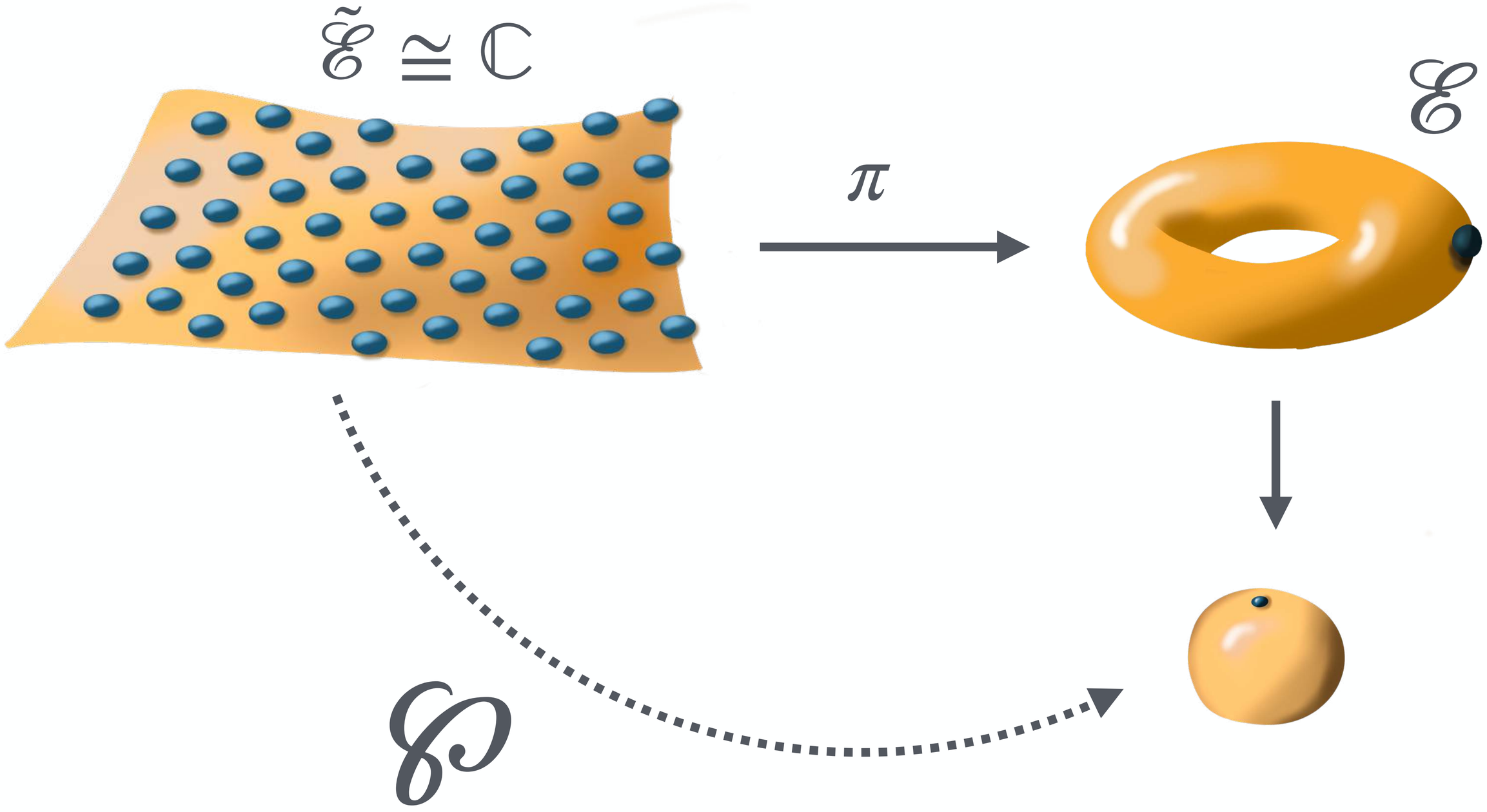
(x, y)



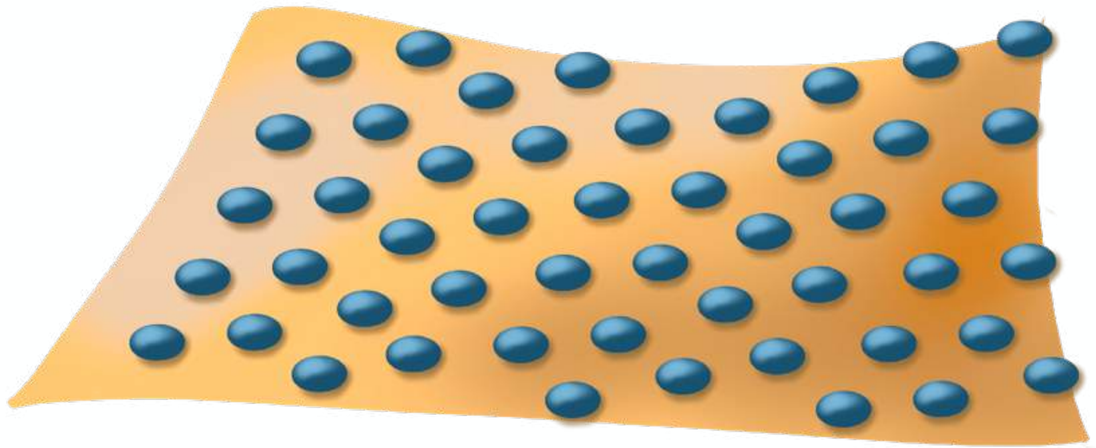
$\mathbb{C}\mathrm{P}^1$

x



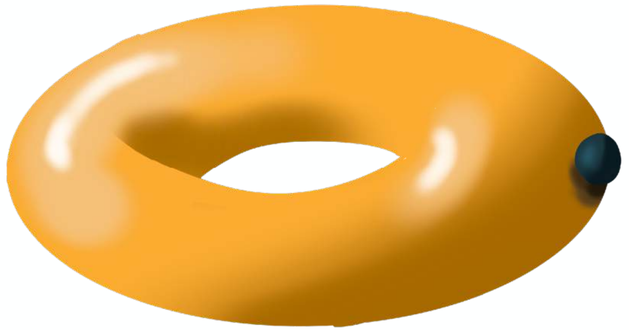

$\tilde{\mathscr{E}} \cong \mathbb{C}$
π
$\mathscr{E}$
$\mathscr{C}$

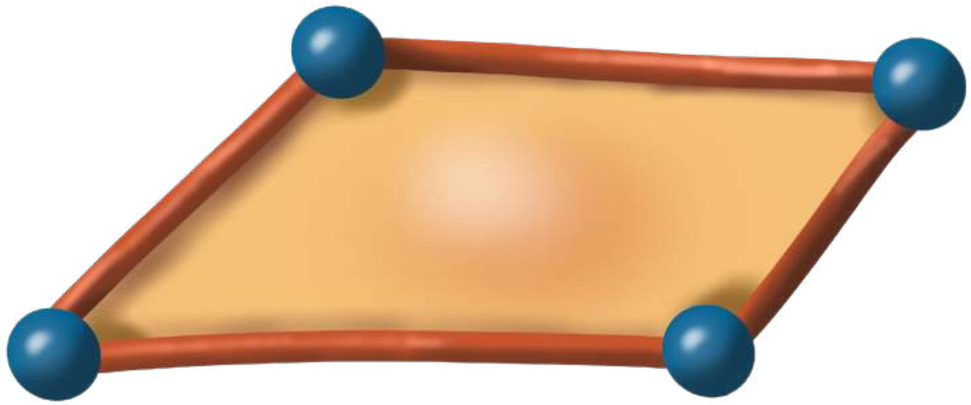
$\tilde{\mathscr{E}} \cong \mathbb{C}$



$(\wp, \wp')$

$\mathscr{E}$

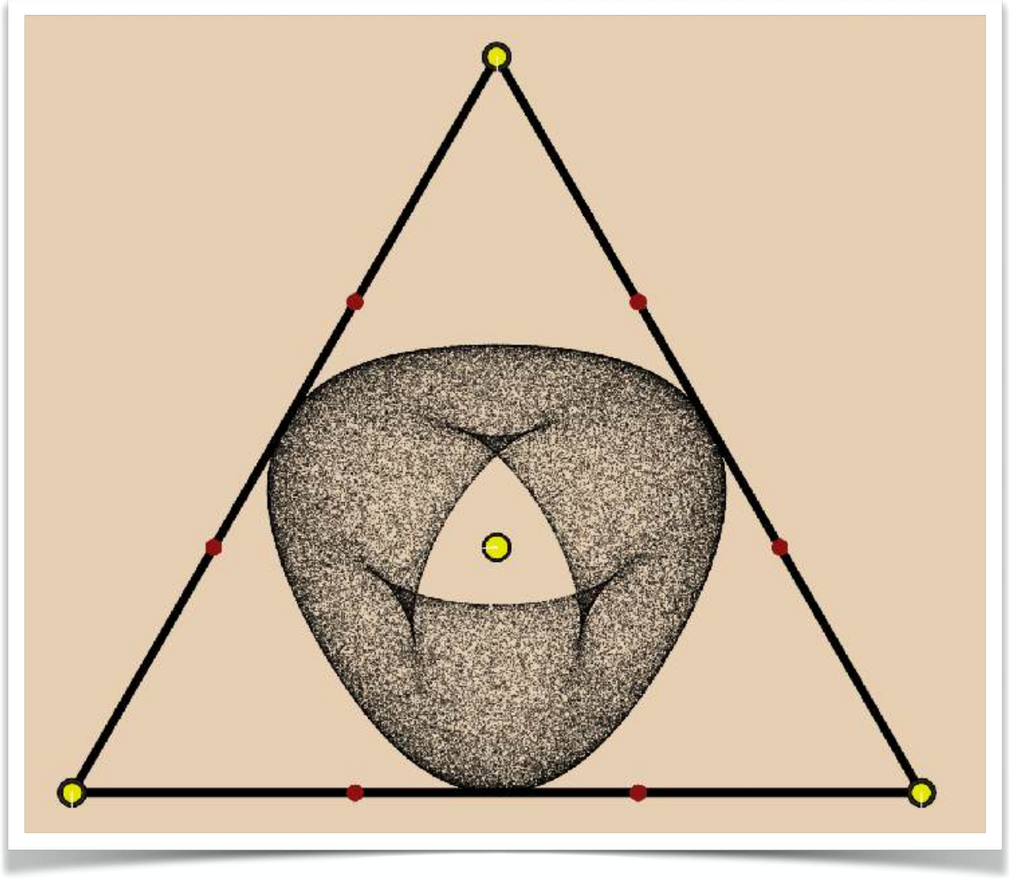




The group law here is transparent: its addition mod the lattice!

chessapig.github.io/code/CP2

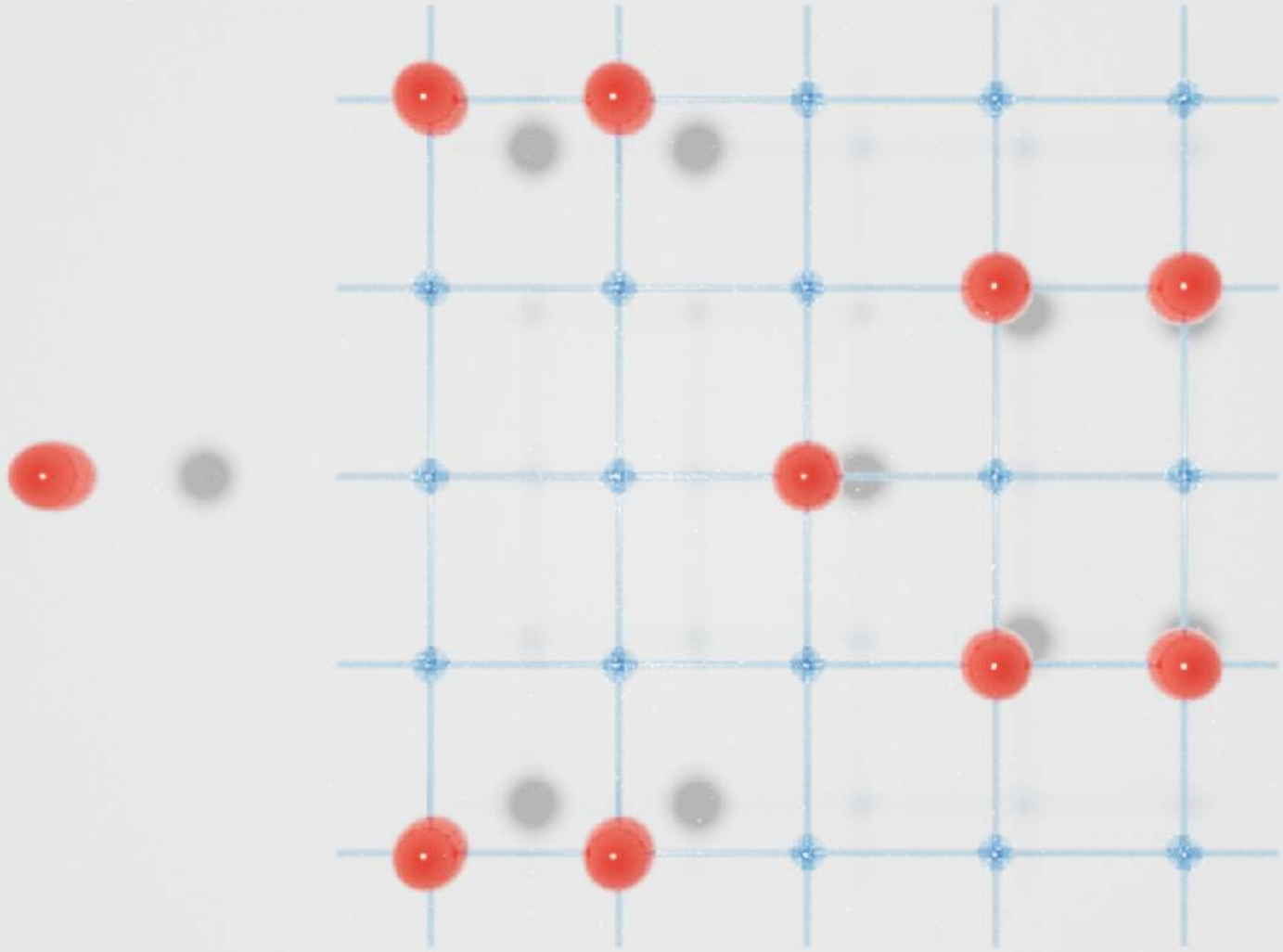
Elliot Kienzle



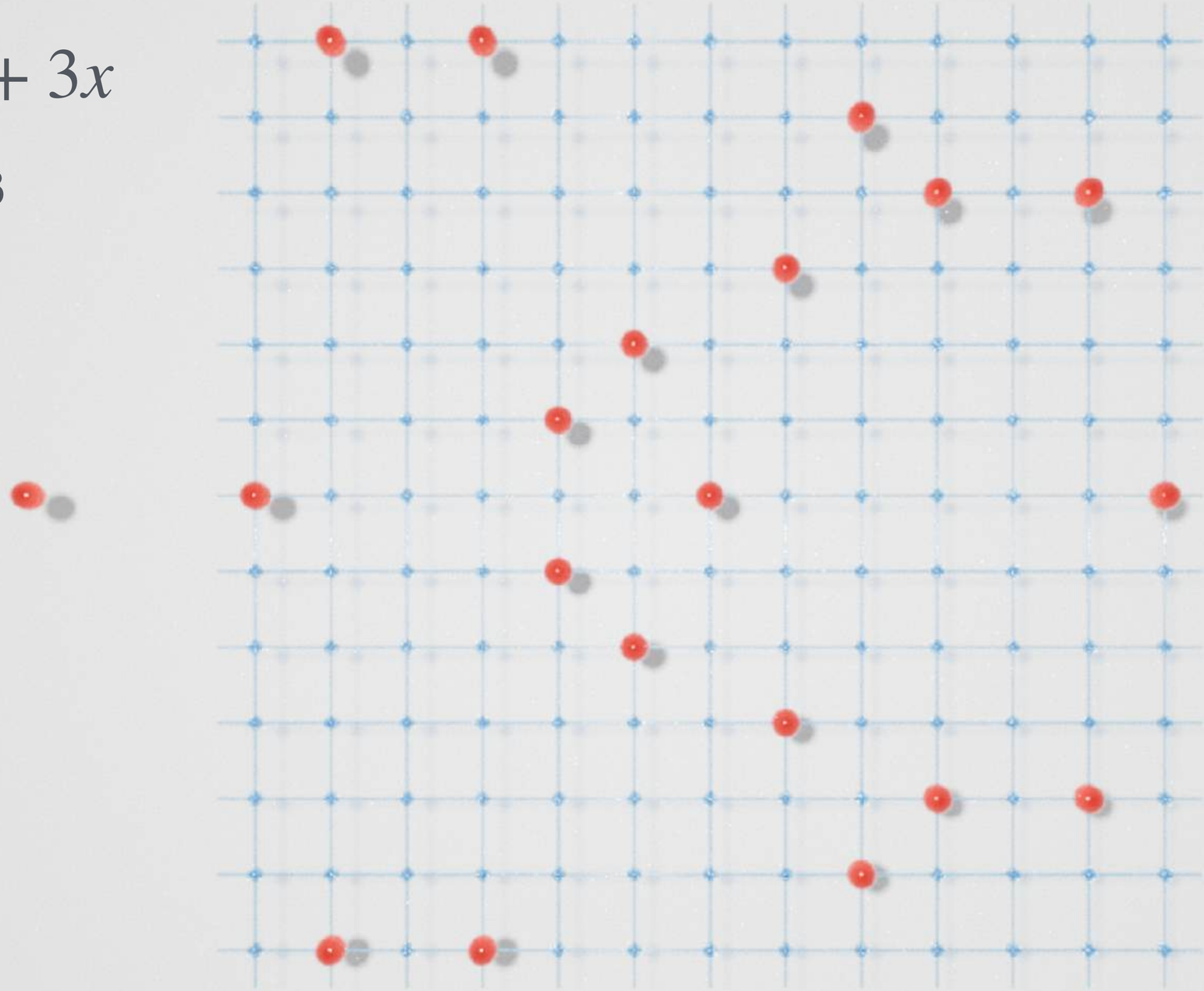
The best pictures of curves in $\mathbb{C}\mathrm{P}^2$ *that I have ever seen*

III Elliptic curves over Finite Fields

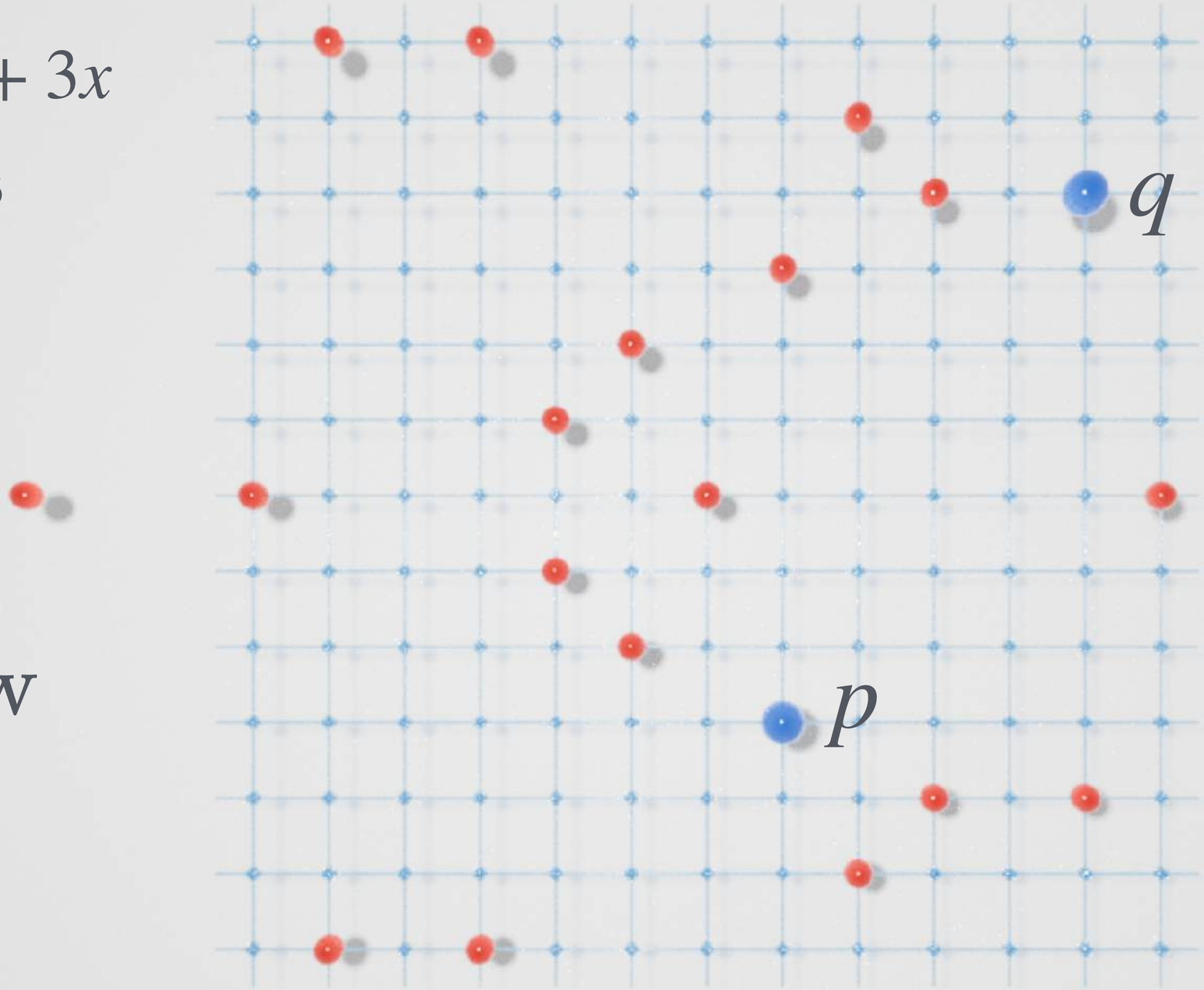
The curve $y^2 = x^3 + 3x$ mod 5, over $\mathbb{F}_5$



The curve $y^2 = x^3 + 3x$ mod 5, over $\mathbb{F}_{13}$

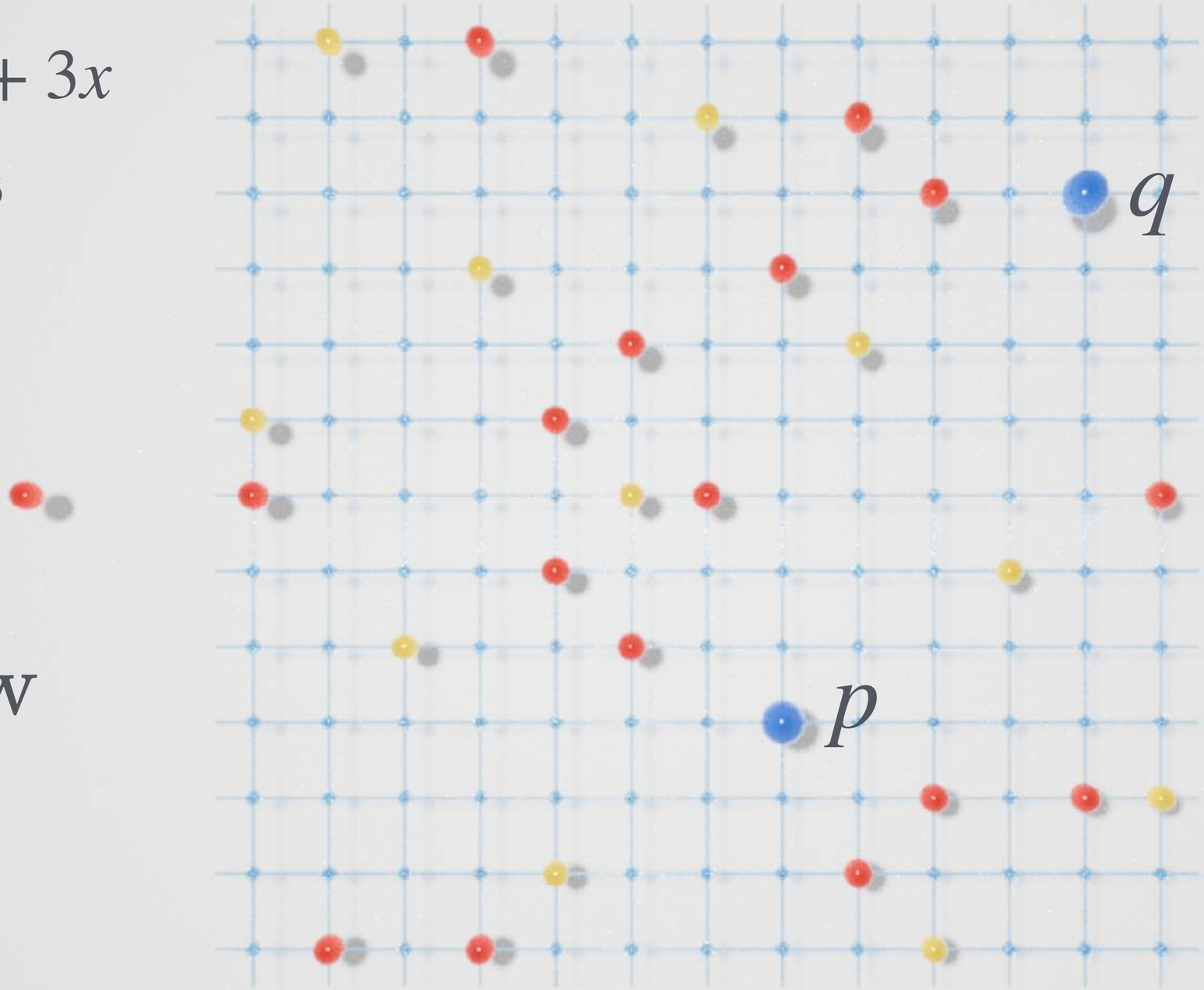


The curve $y^2 = x^3 + 3x$ mod 5, over $\mathbb{F}_{13}$



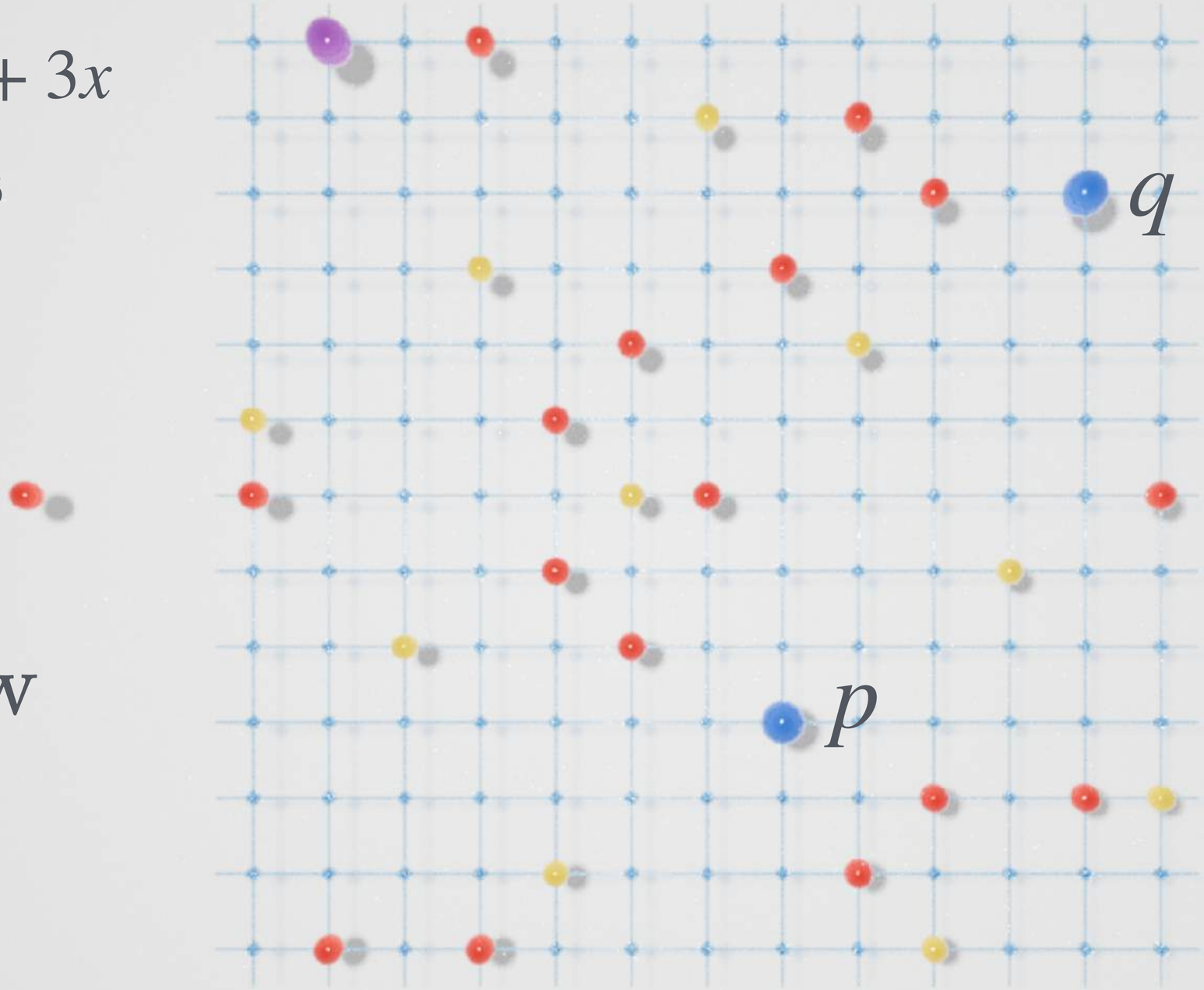
The group law follows the same algebra

The curve $y^2 = x^3 + 3x$ mod 5, over $\mathbb{F}_{13}$



The group law follows the same algebra

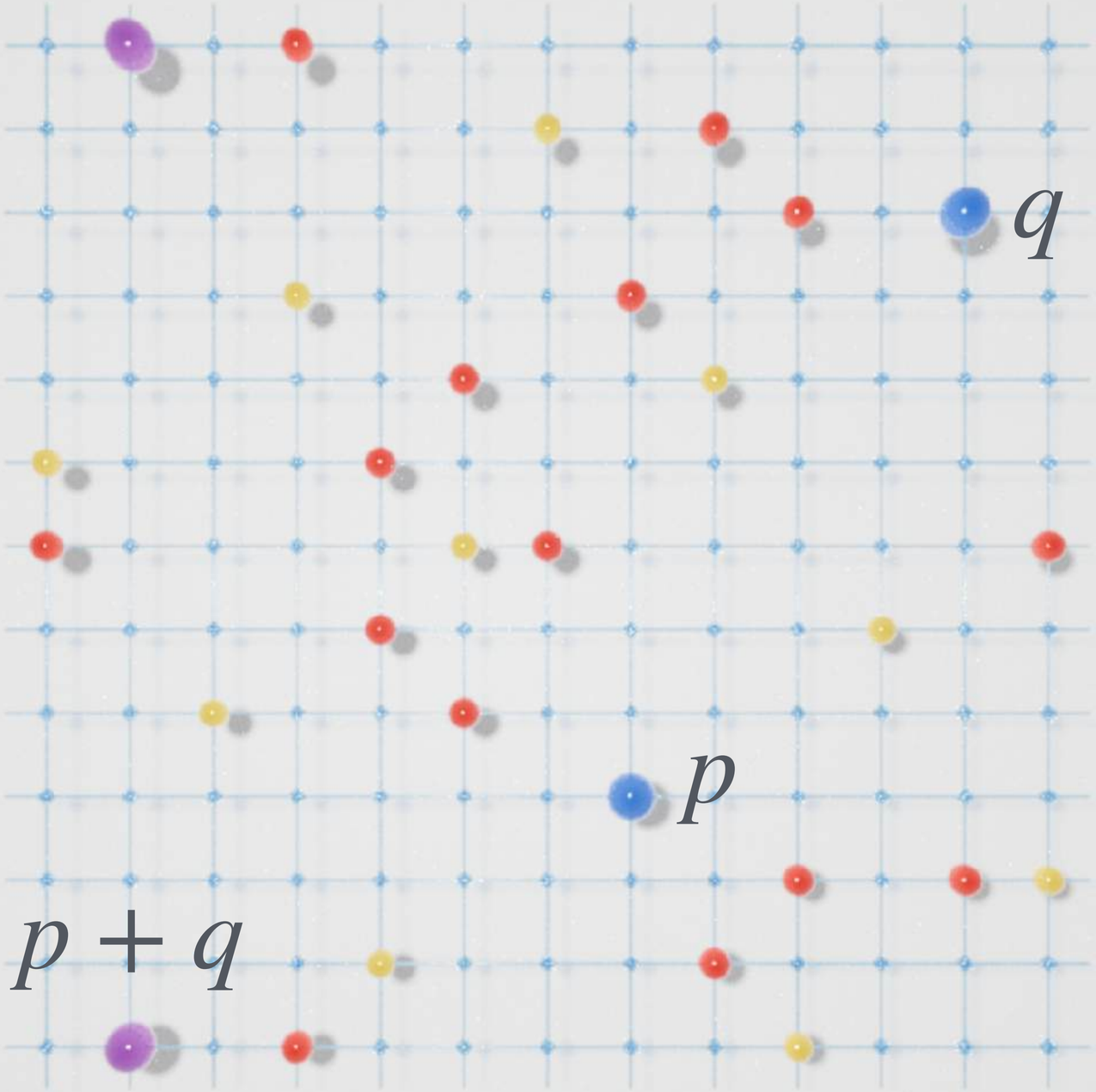
The curve $y^2 = x^3 + 3x$ mod 5, over $\mathbb{F}_{13}$



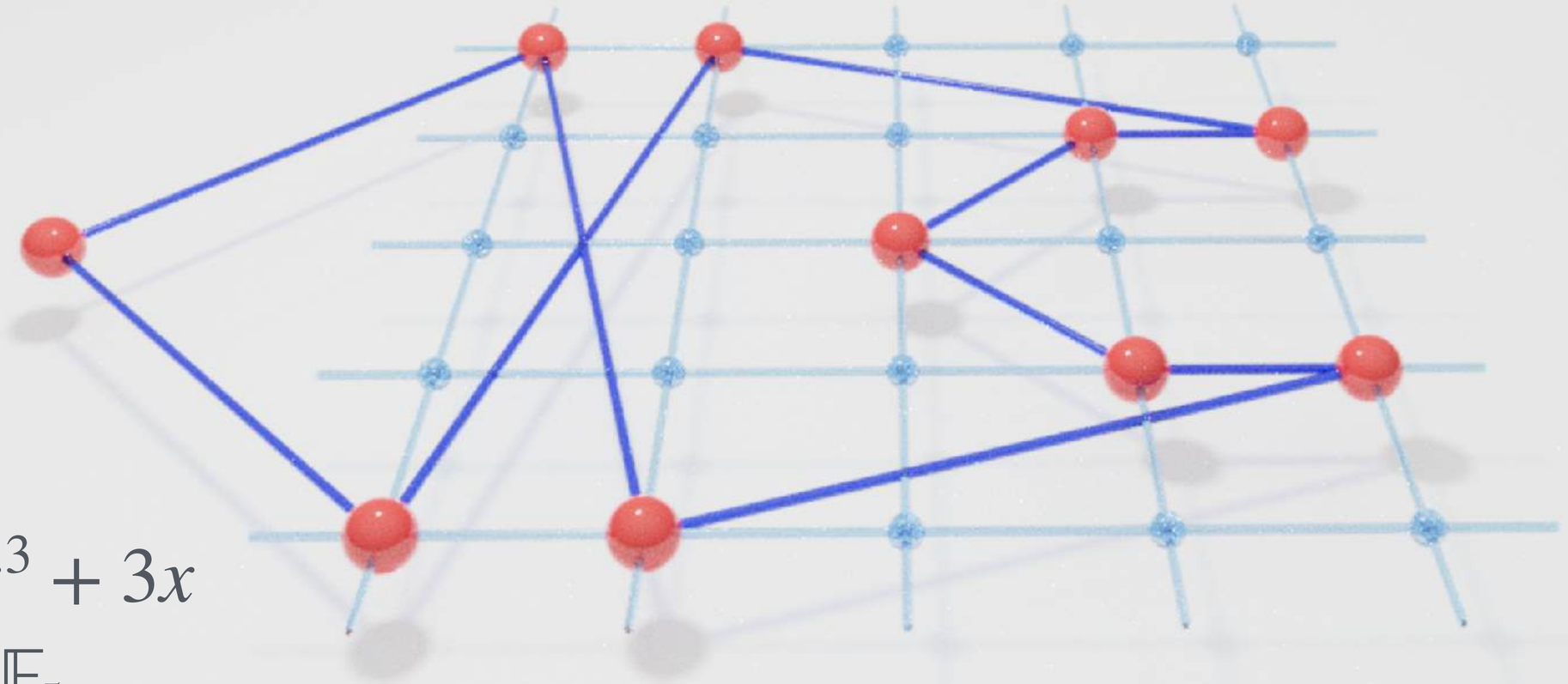
The group law follows the same algebra

The curve $y^2 = x^3 + 3x$ mod 5, over $\mathbb{F}_{13}$

The group law follows the same algebra



And again the group structure is rather unrelated to the underlying space

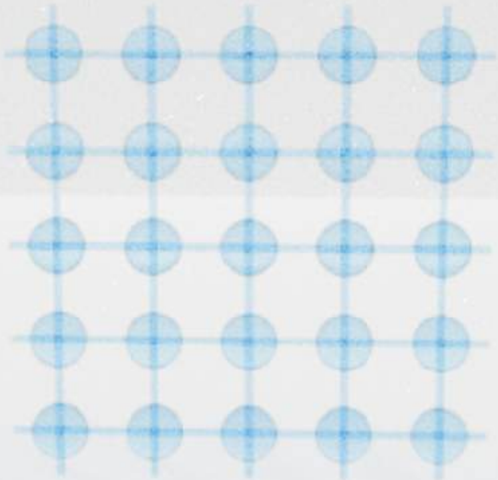


The curve $y^2 = x^3 + 3x$ mod 5, over $\mathbb{F}_5$

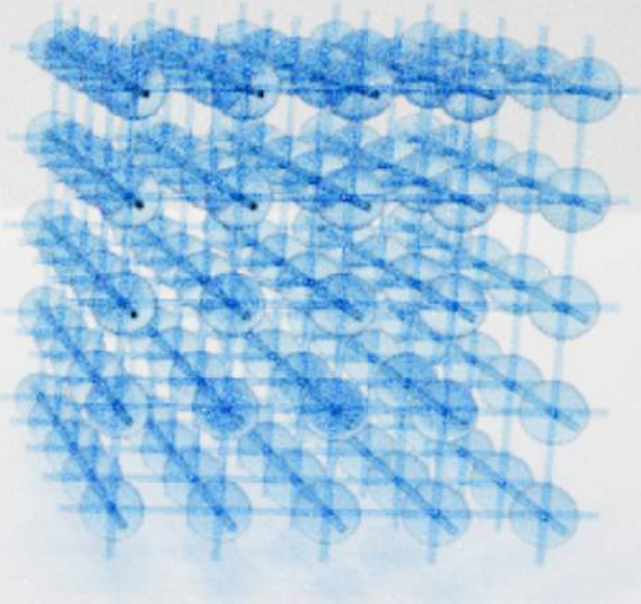
However…even such pictures only really work for fields of prime order.

$\mathbb{F}_5$

$\mathbb{F}_{25}$

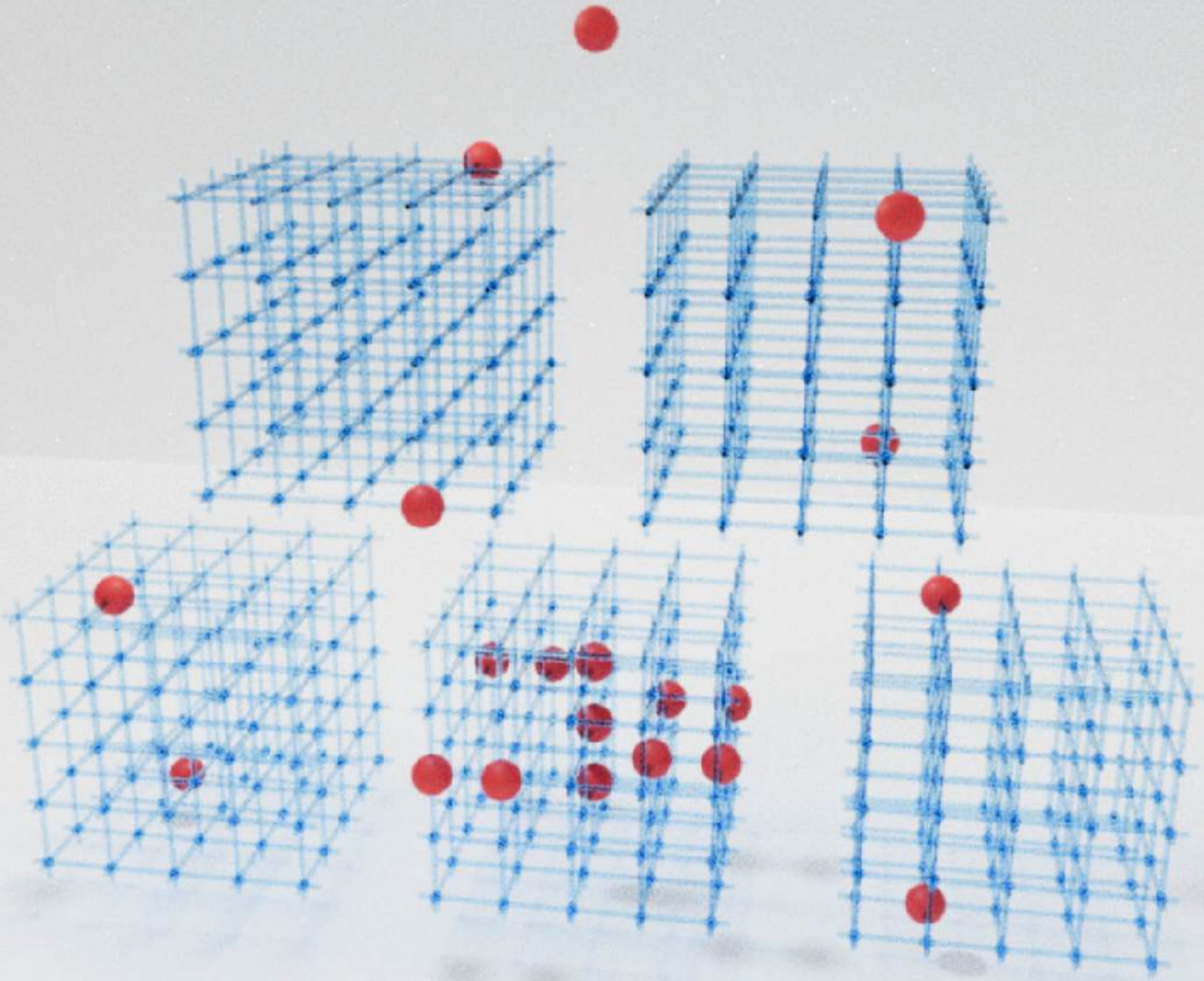


$\mathbb{F}_{125}$



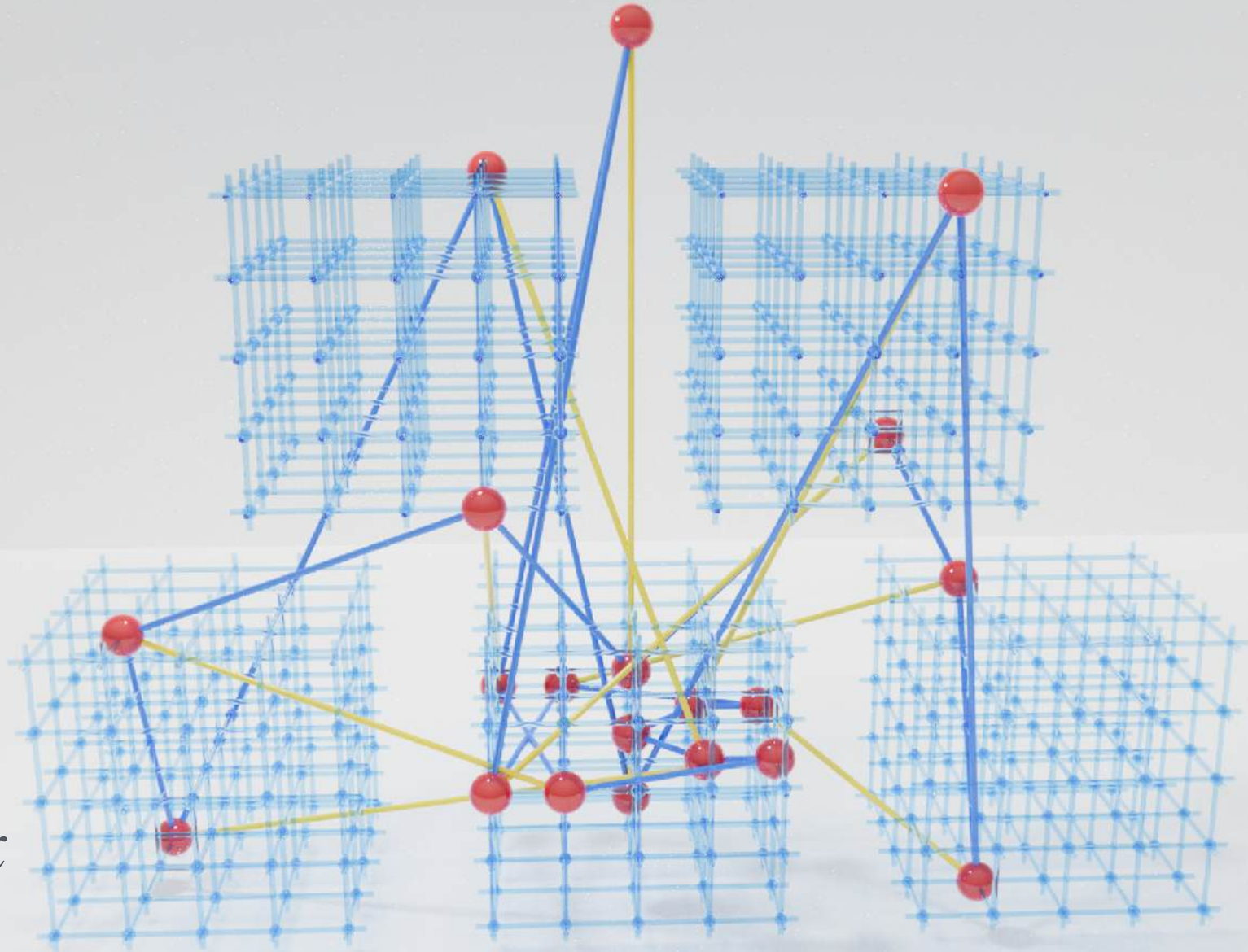
The field $\mathbb{F}_{p^n}$ is an n-dimensional vector space over $\mathbb{F}_p$

However…even such pictures only really work for fields of prime order.



The curve $y^2 = x^3 + 3x$ mod 5, over $\mathbb{F}_{25}$

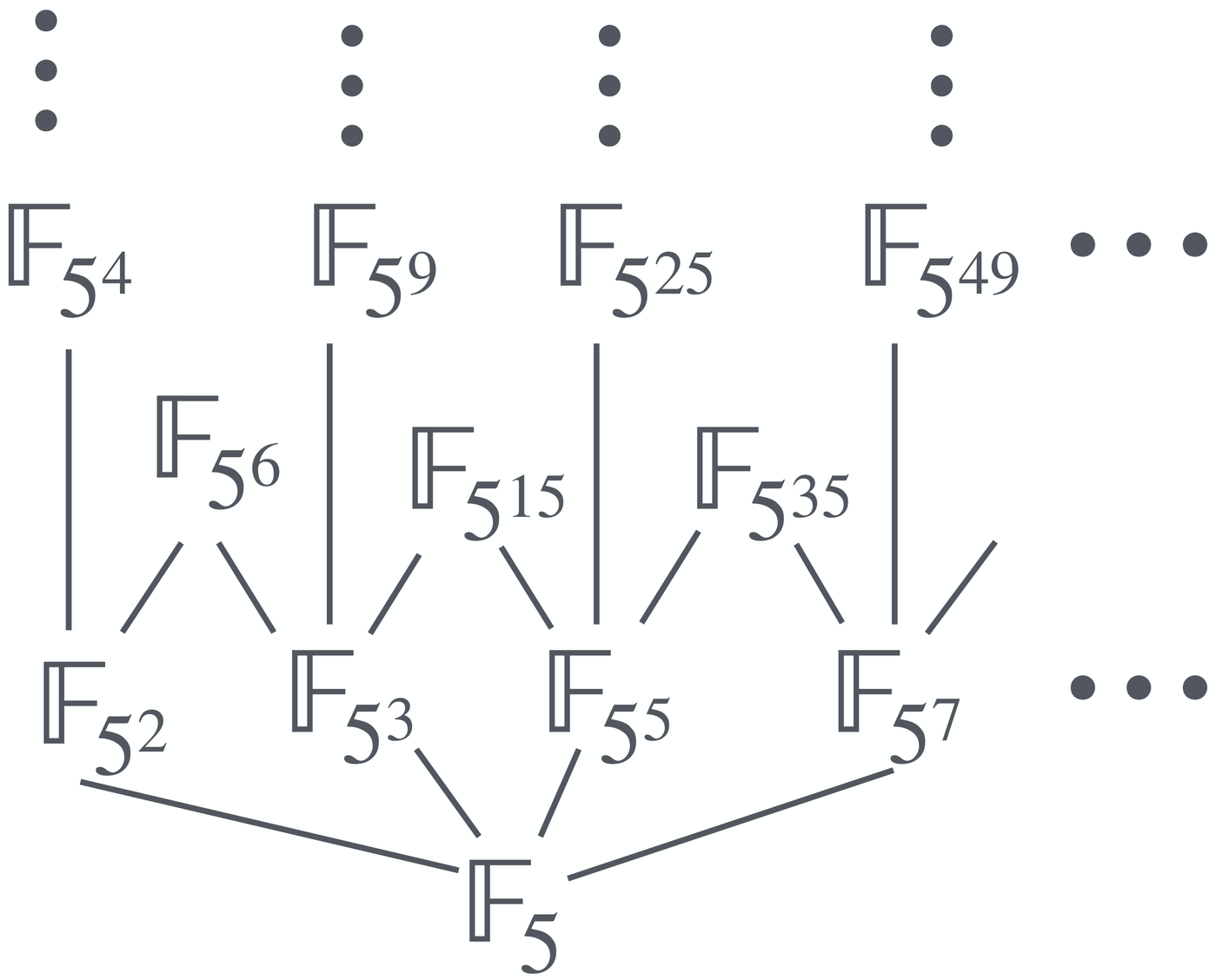
However…even such pictures only really work for fields of prime order.



The curve $y^2 = x^3 + 3x$ mod 5, over $\mathbb{F}_{25}$

However…even such pictures only really work for fields of prime order.

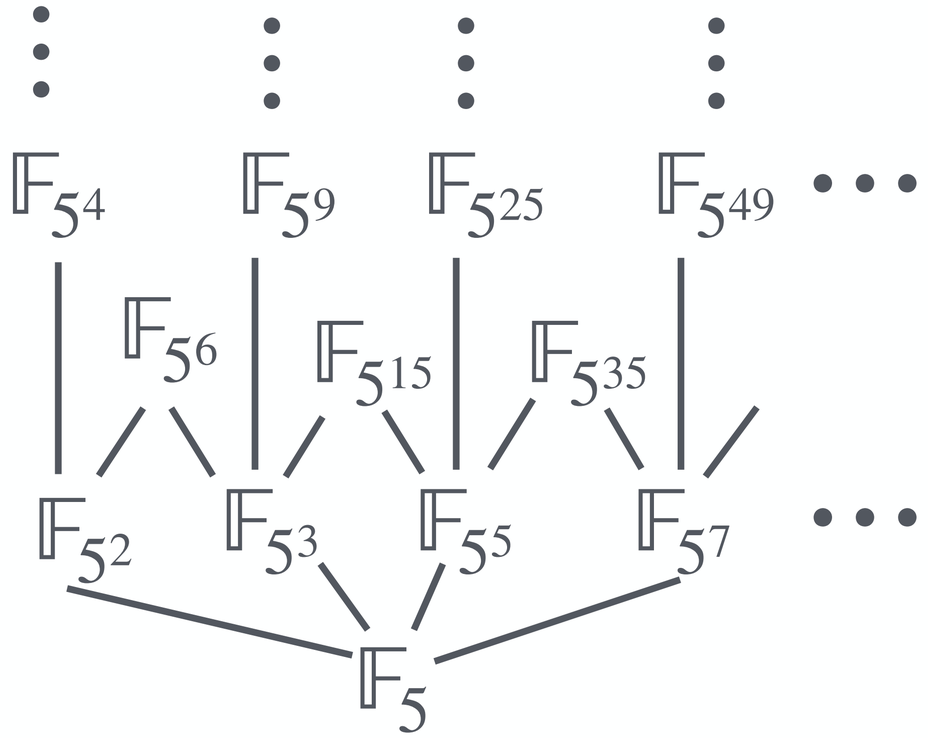
…..And there are many other finite fields



Visualization Challenge:

Can we find a “nice” visualization of finite Elliptic curves?

- The group law is visible
- We can see curves over extension fields without the dimension exploding



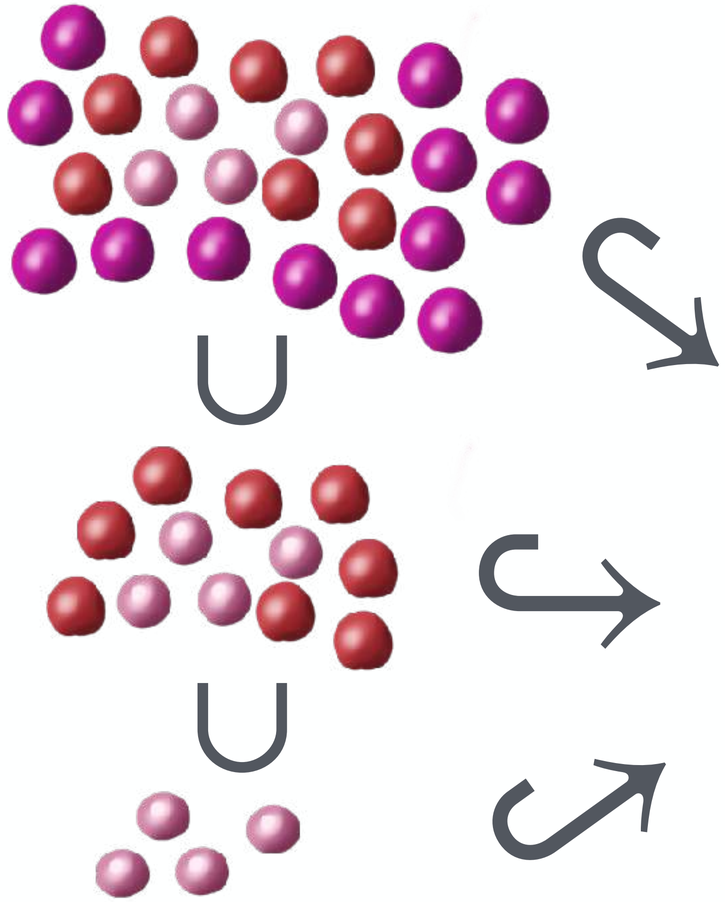
IV Lifting to a Geometric World

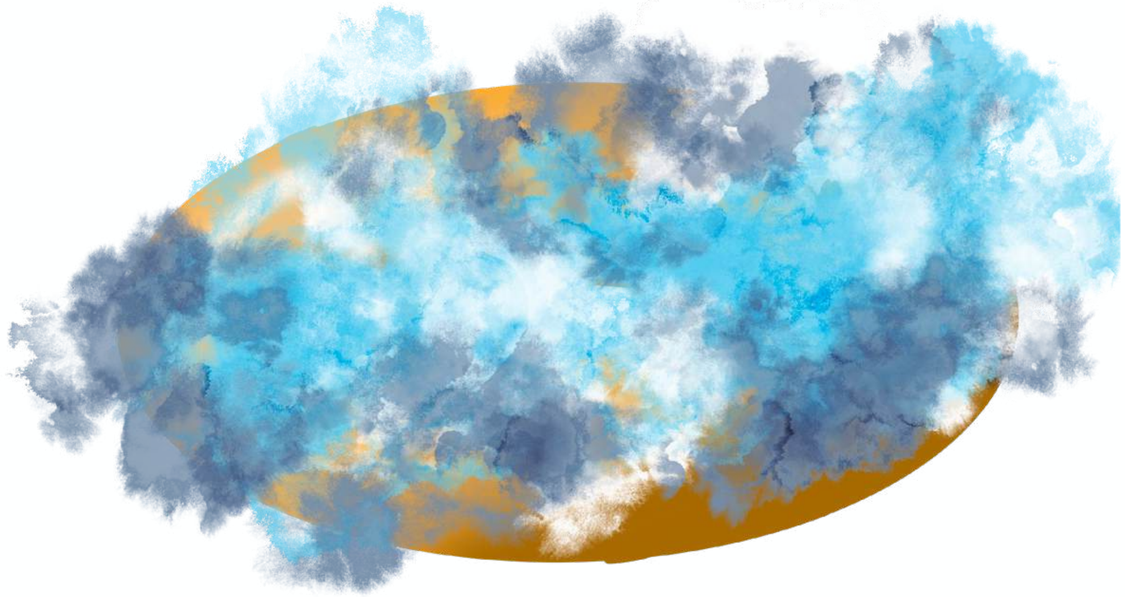
Finding a uniform home for all

$\mathscr{E}/\mathbb{F}_{p^4}$

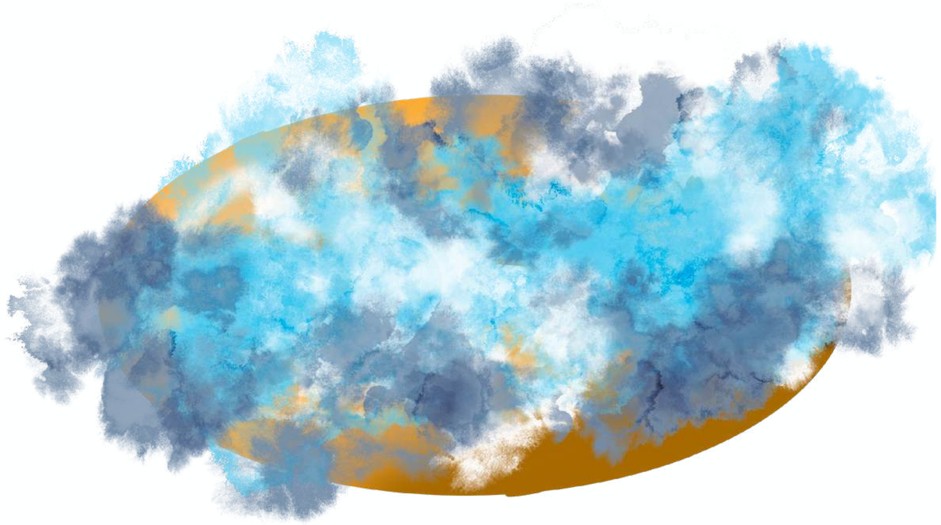
$\mathscr{E}/\mathbb{F}_{p^2}$

$\mathscr{E}/\mathbb{F}_{p}$

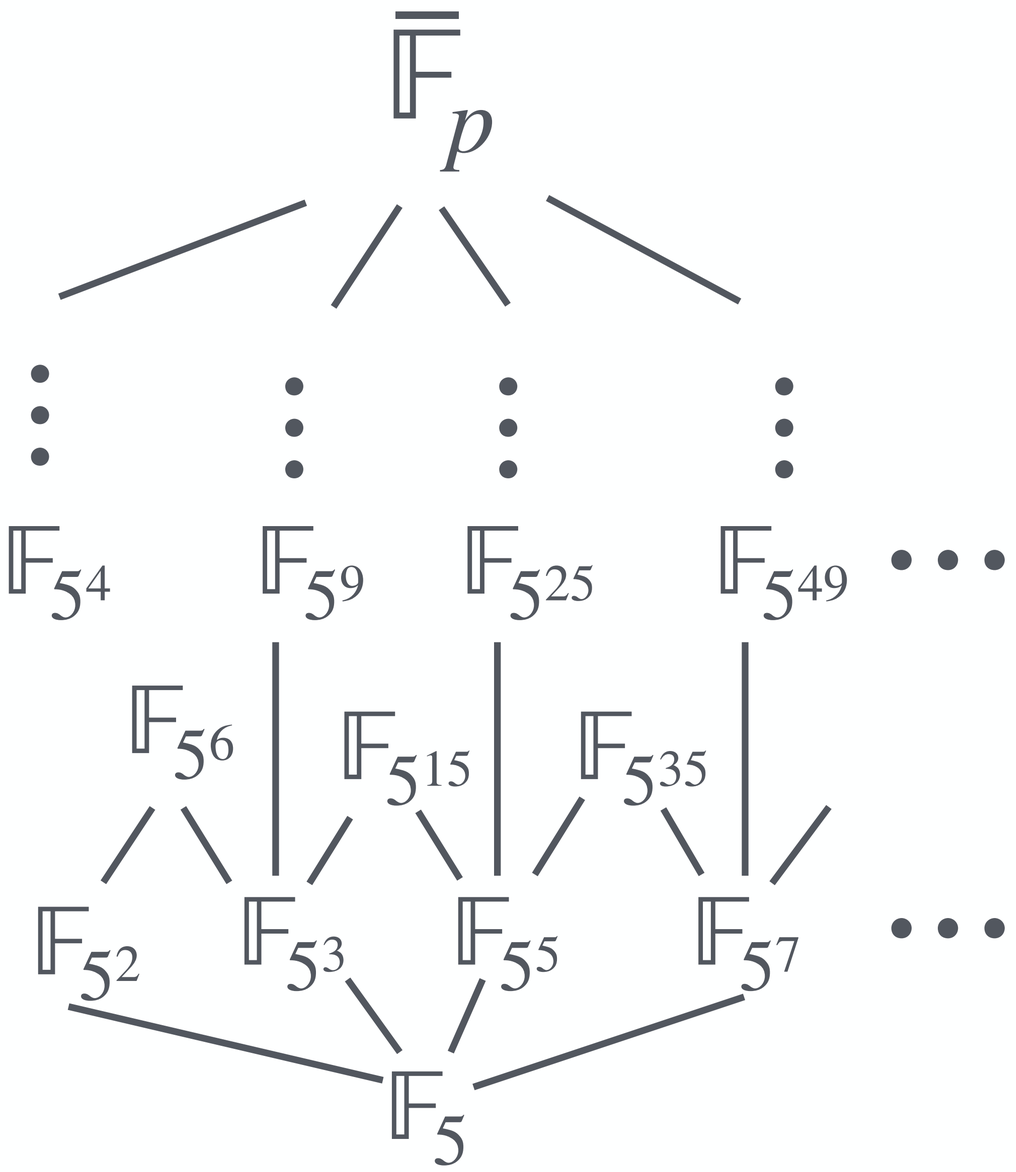




The curve over the algebraic closure is a natural candidate



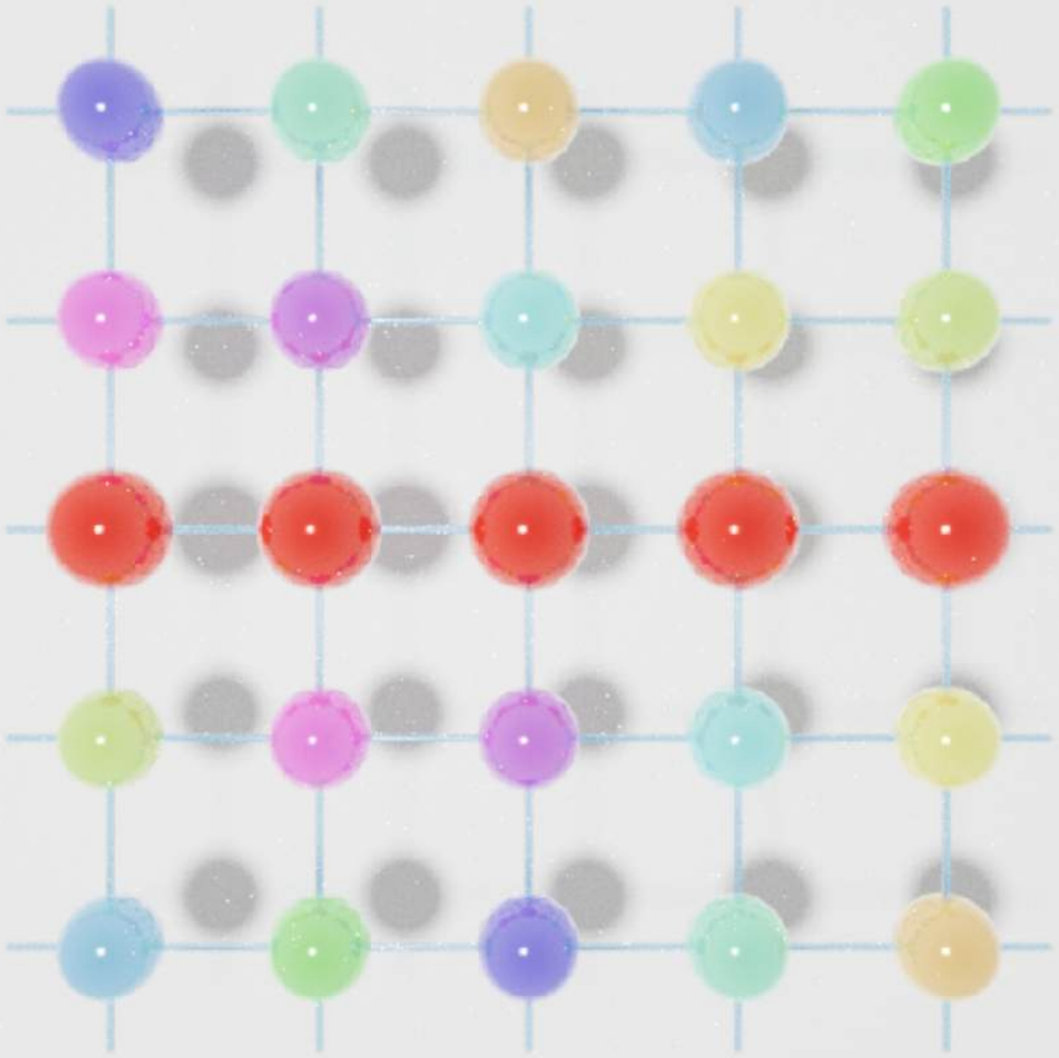
$\mathscr{E}/\overline{\mathbb{F}}_p$



The Galois theory of these fields is determined by Frobenius

The Frobenius Map

$$(x, y) \mapsto (x^p, y^p)$$

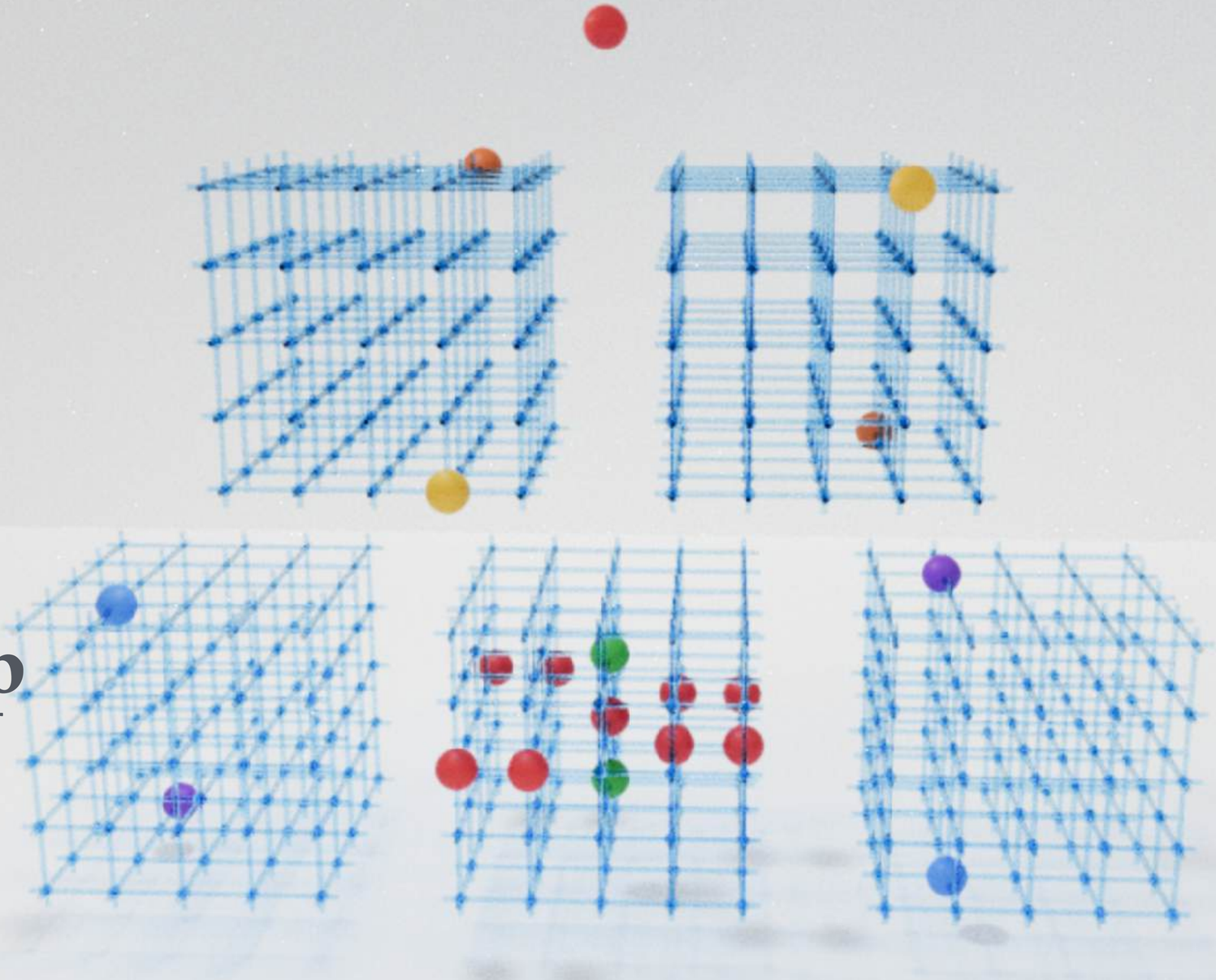


The field $\mathbb{F}_{25}$ as a vector space over $\mathbb{F}_5$

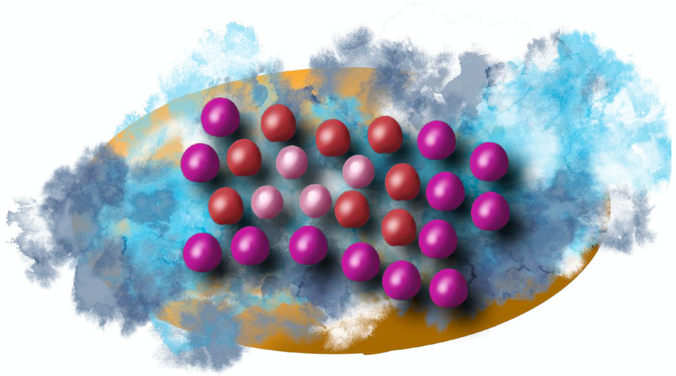
This extends to the elliptic curves

The Frobenius Map

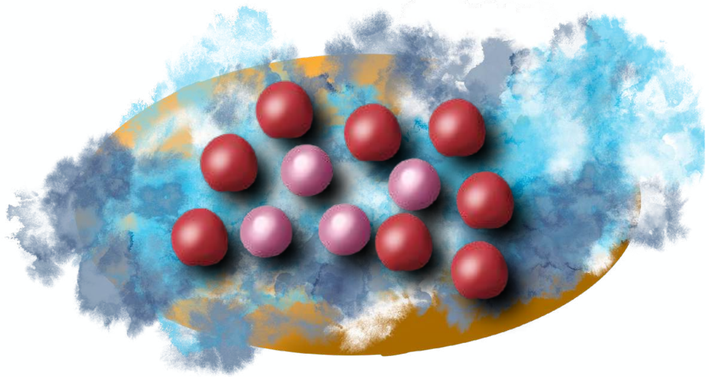
$$(x, y) \mapsto (x^p, y^p)$$



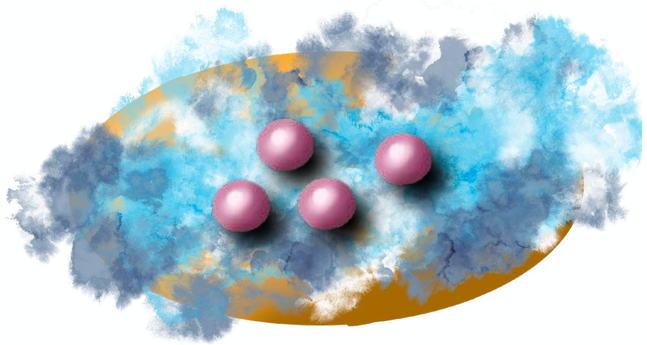
The curve $y^2 = x^3 + 3x \bmod 5$, over $\mathbb{F}_{25}$



$\mathscr{E}/\mathbb{F}_{p^4}$ is the fixed points of ϕ^4



$\mathscr{E}/\mathbb{F}_{p^2}$ is the fixed points of ϕ^2

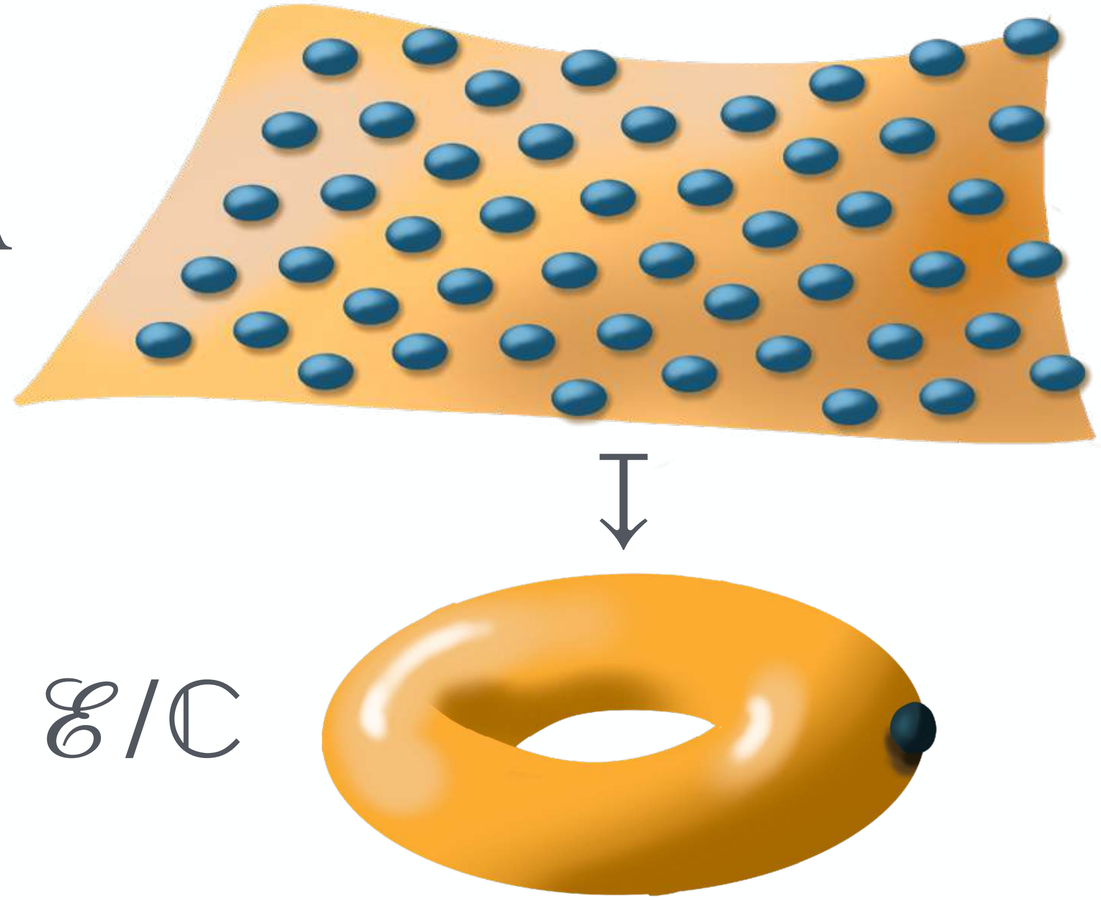


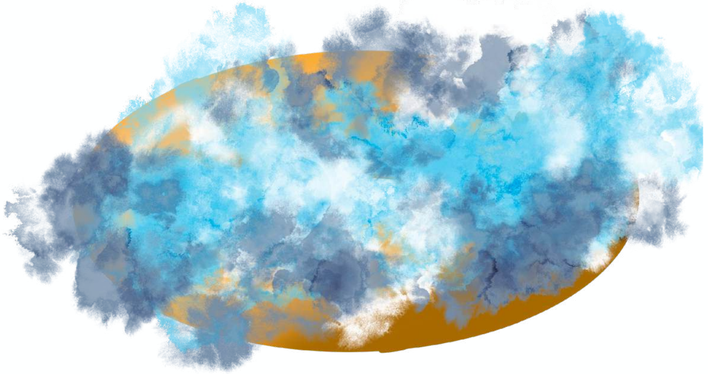
$\mathscr{E}/\mathbb{F}_{p}$ is the fixed points of ϕ

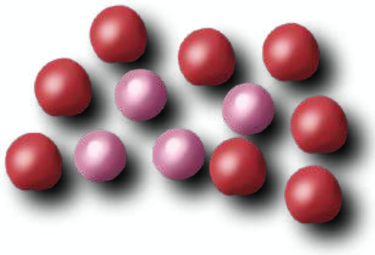
Realizing the algebraic closure

$$\mathbb{Z}^{\mathrm{alg}}/\mathfrak{P} \cong \mathbb{F}_p$$

But $\mathbb{Z}^{\mathrm{alg}}$ is a subset of $\mathbb{C}$: so maybe we can start with a complex elliptic curve, and reduce some of its points mod p?





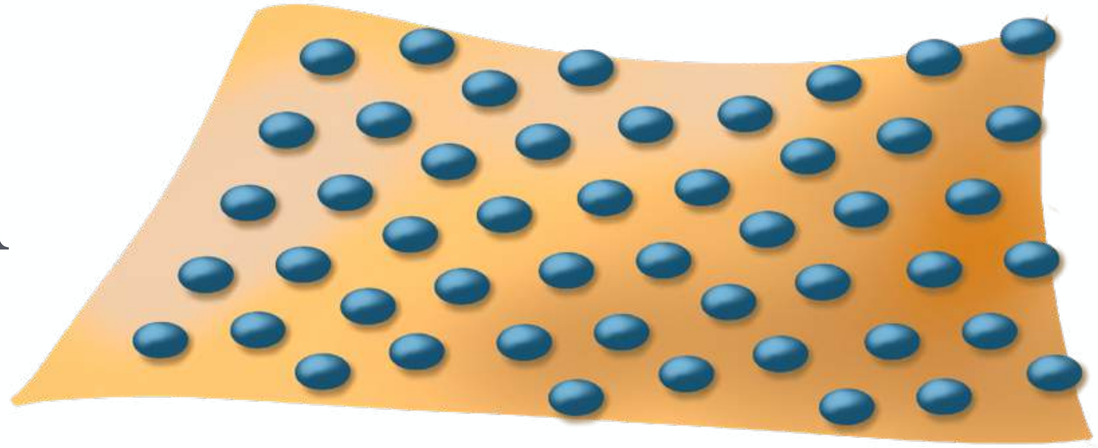


The Big Picture

Lift frobenius and find the fixed points

The Big Picture

$\mathbb{C}/\Lambda$



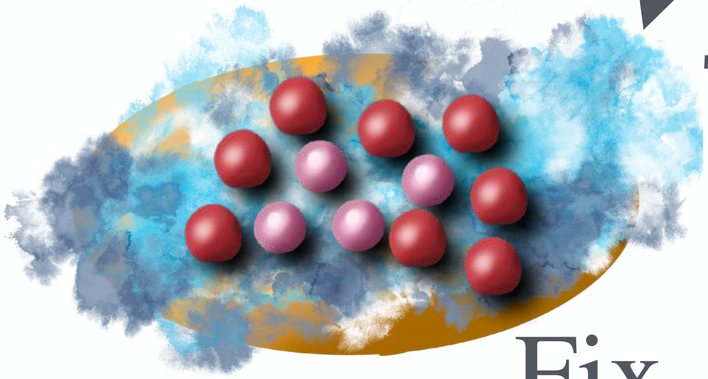
$\tilde{\phi}$

$$z + \Lambda \mapsto \alpha z + \Lambda$$

The ambient curve has complex multiplication

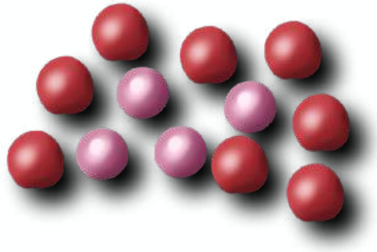
$\mathscr{E}/\mathbb{F}_p$

ϕ

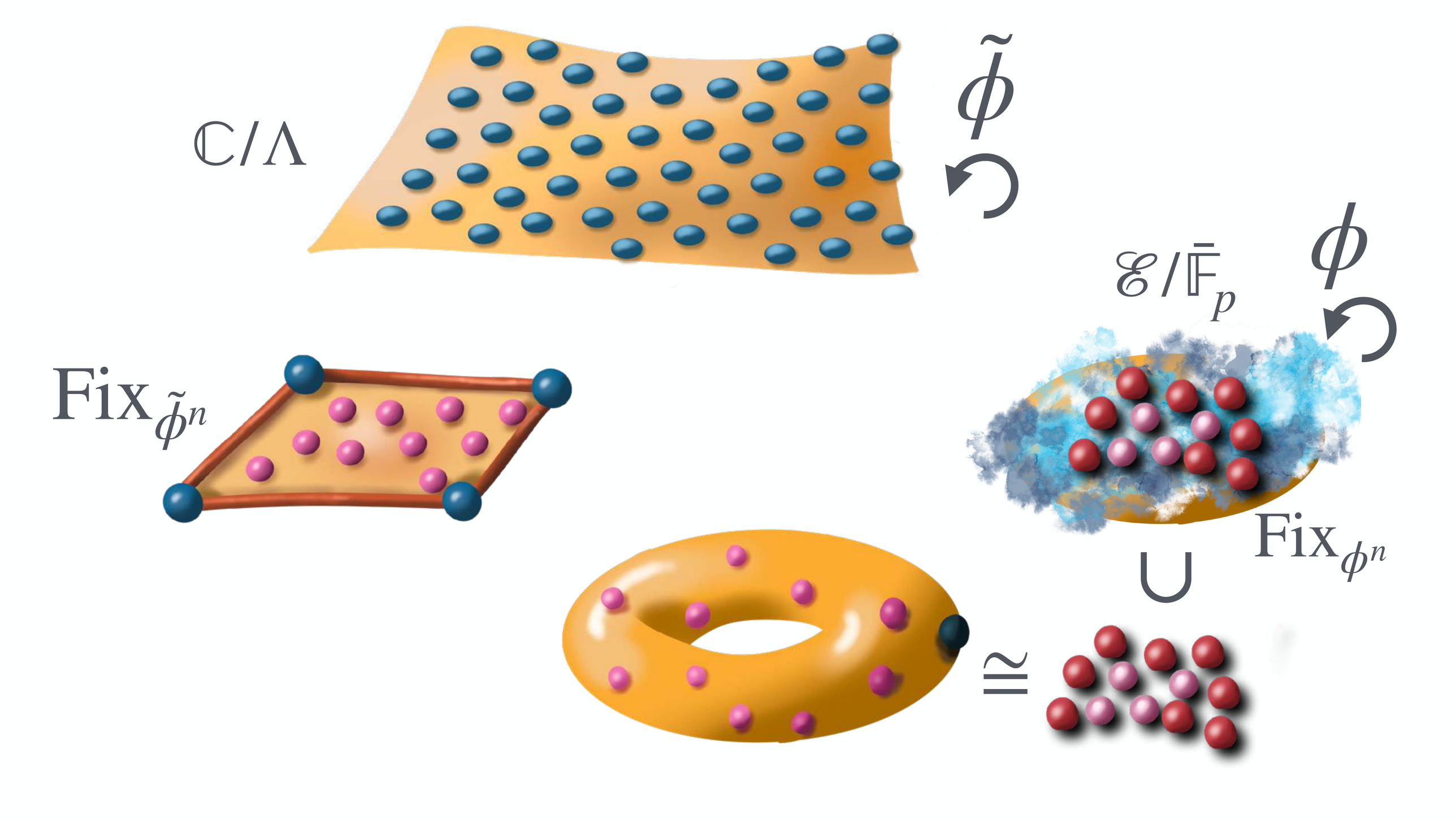


Fix_{ϕ^n}

$\cup$



$\mathscr{E}/\mathbb{F}_{p^n}$


$\mathbb{C}/\Lambda$
$\tilde{\phi}$
$\mathrm{Fix}_{\tilde{\phi}^n}$
$\mathscr{E}/\mathbb{F}_p$
ϕ
Fix_{ϕ^n}
$\cong$

Theorem

We can do this

Every elliptic curve mod p can be embedded in an elliptic curve over $\mathbb{C}$ with complex multiplication.

Given a curve $\mathscr{E}$ over $\mathbb{F}_{p^n}$, the work of Deuring provides a lattice $\Lambda \subset \mathbb{C}$ and a map $\tilde{\phi} : z + \Lambda \mapsto \alpha z + \Lambda$ such that the fixed points of $\tilde{\phi}^n$ reduce mod p isomorphically to $\mathscr{E}$.

Theorem (Hajouji, T~) 26

Equivalence of categories

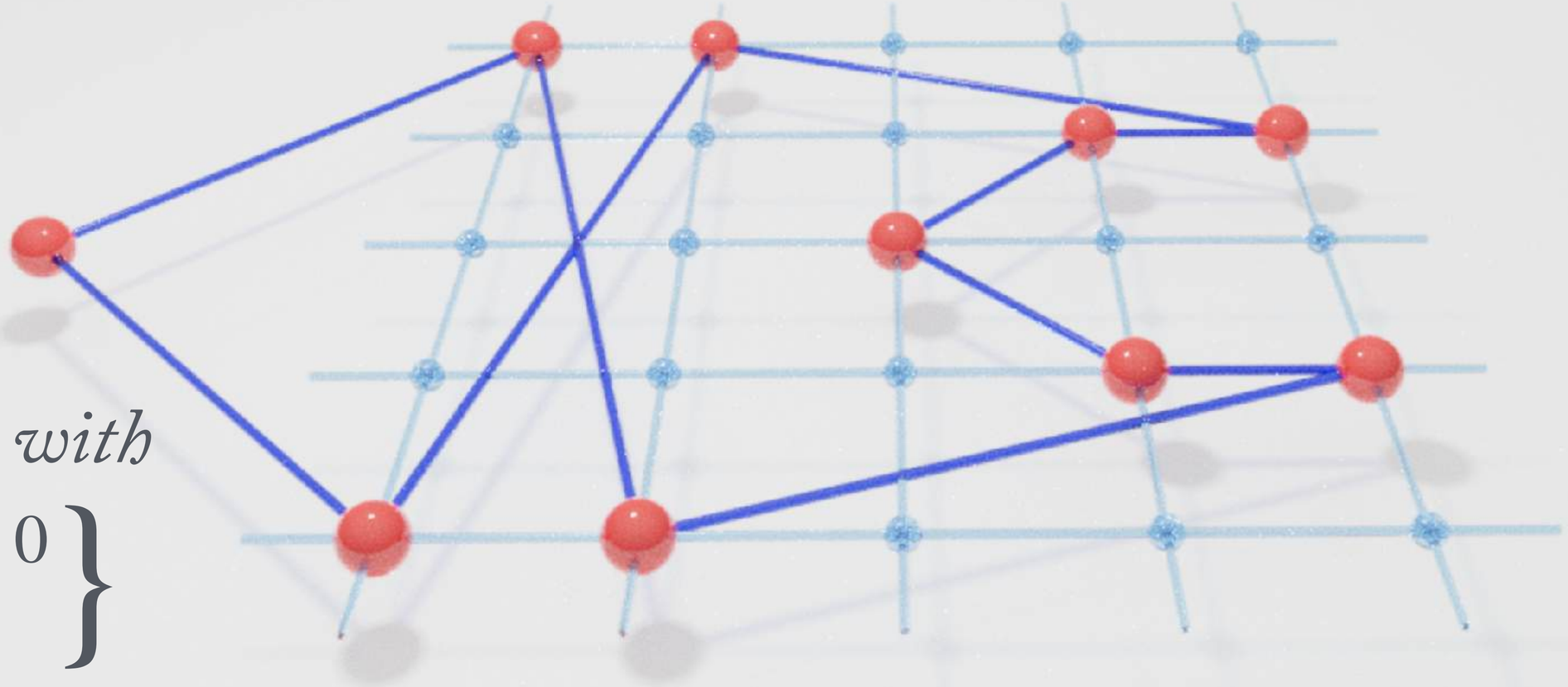
The category of lattices with an endomorphism of degree p is equivalent to the category of elliptic curves over $\mathbb{F}_p$

Fix a pair (a, p) and a root α of $x^2 + ax + p$, and form the category of $\mathscr{L}_\alpha$ lattices with complex multiplication by α. Then this is equivalent to the category of elliptic curves over $\mathbb{F}_p$ whose trace of Frobenius is a.

And, we can **compute this equivalence explicitly.**

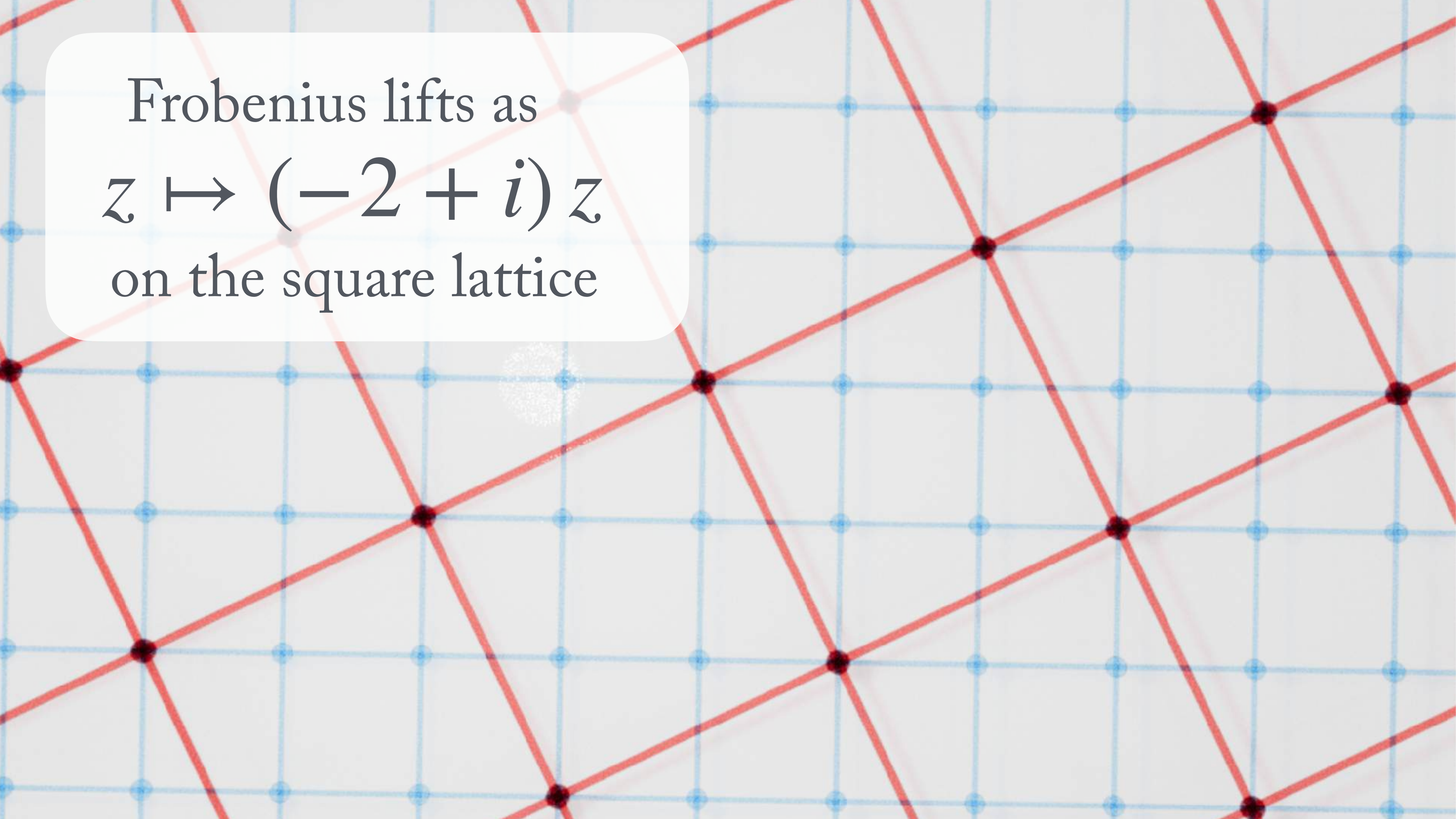
$$y^2 = x^3 + 3x \mod 5$$

Frobenius satisfies
$\phi^2 + 4\phi + 5 = 0$



Search for (Λ, α) *with*

$$\left\{ \begin{array}{c} \alpha^2 + 4\alpha + 5 = 0 \\ \alpha\Lambda \subset \Lambda \end{array} \right\}$$

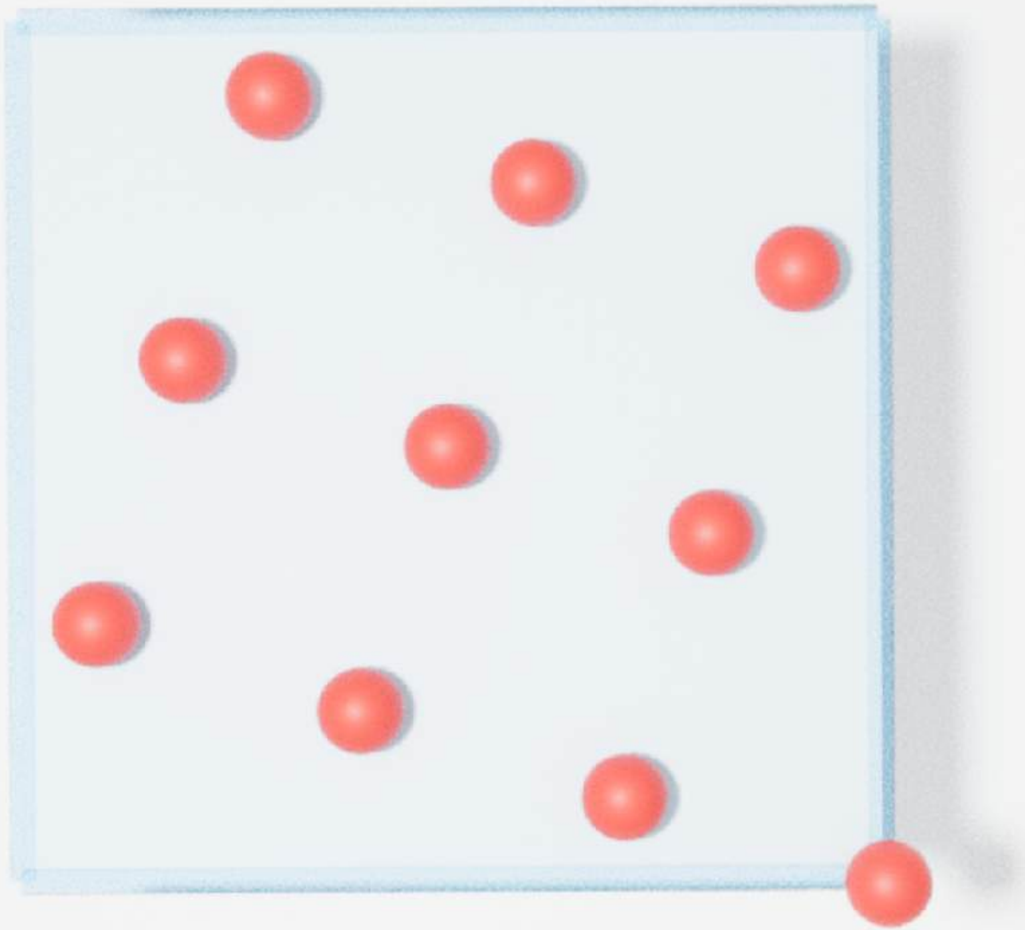

Frobenius lifts as
$z \mapsto (-2+i)\,z$
on the square lattice

$$y^2 = x^3 + 3x \mod 5$$

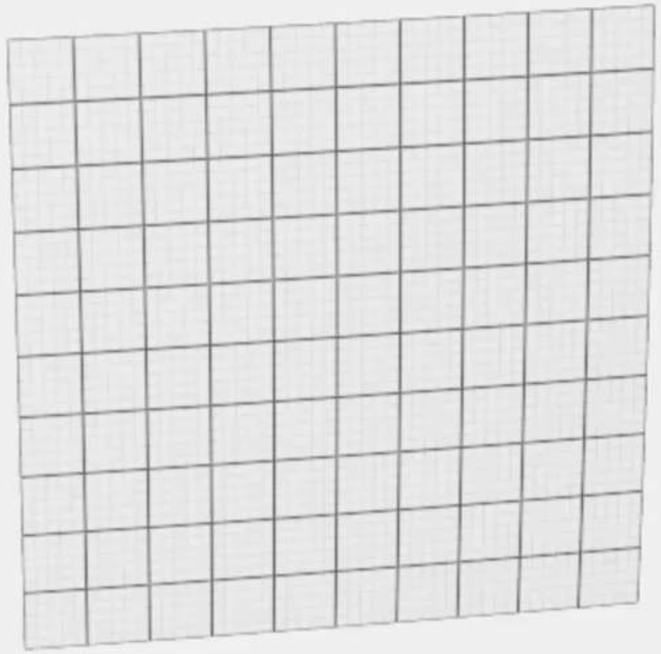
Fixed points of

$z + \Lambda \mapsto (-2 + i)z + \Lambda$

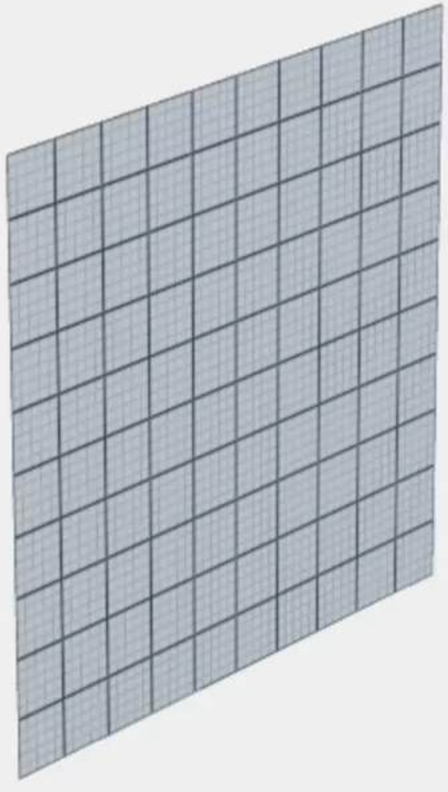
are the $\mathbb{F}_5$ points



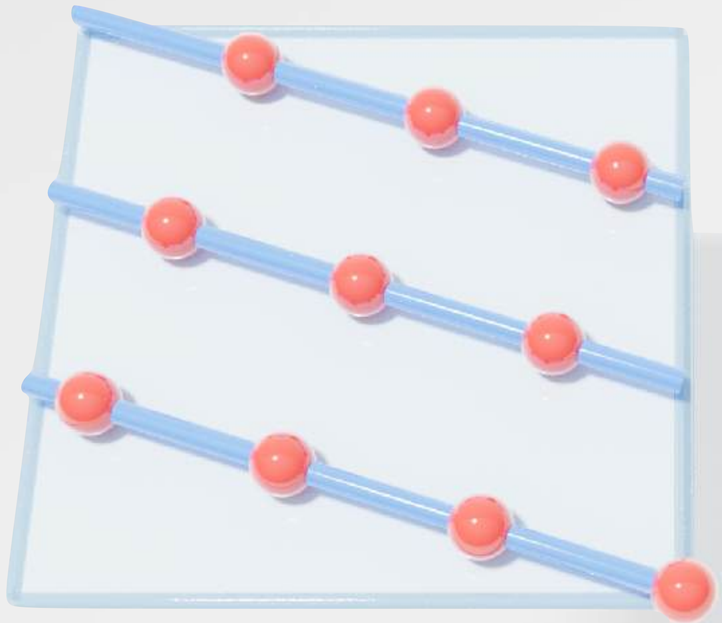
Can’t just roll up the torus arbitrarily: it’ll give the wrong Riemann surface!

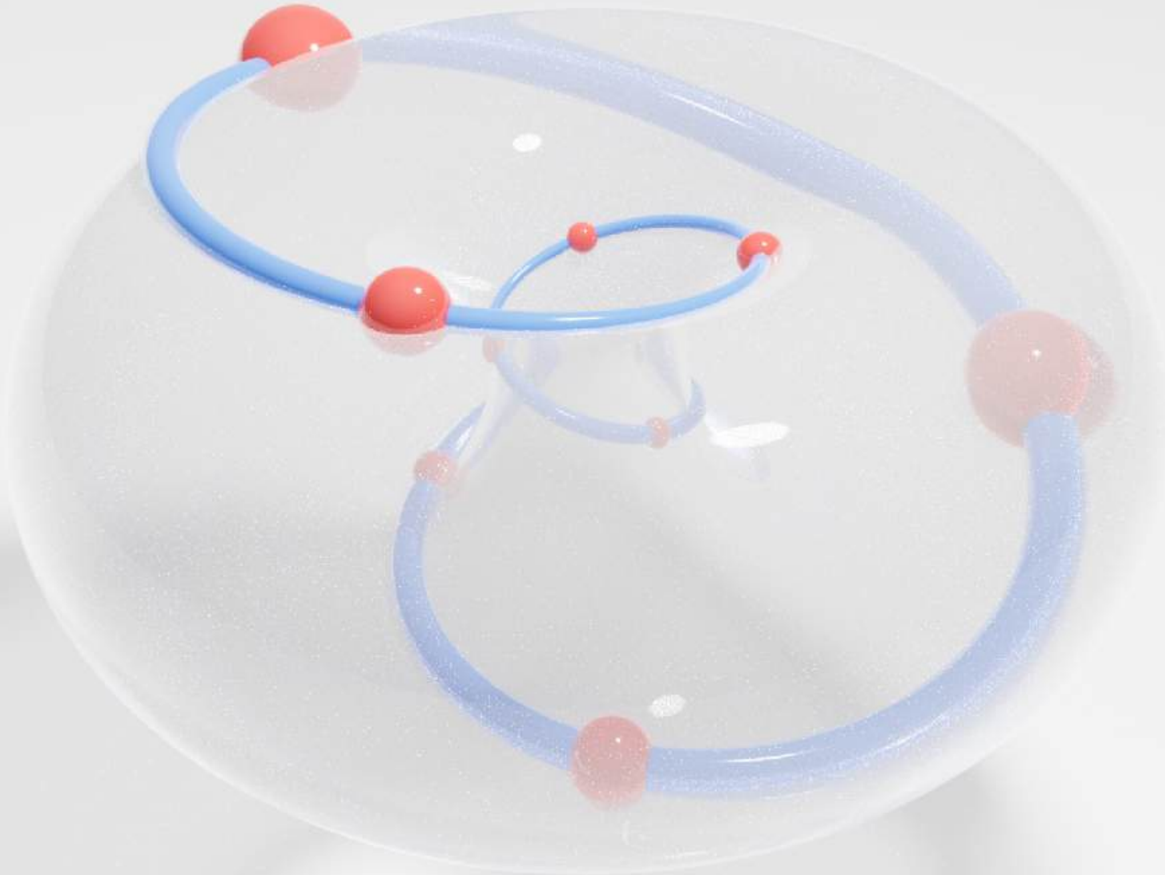


Instead, roll up conformally



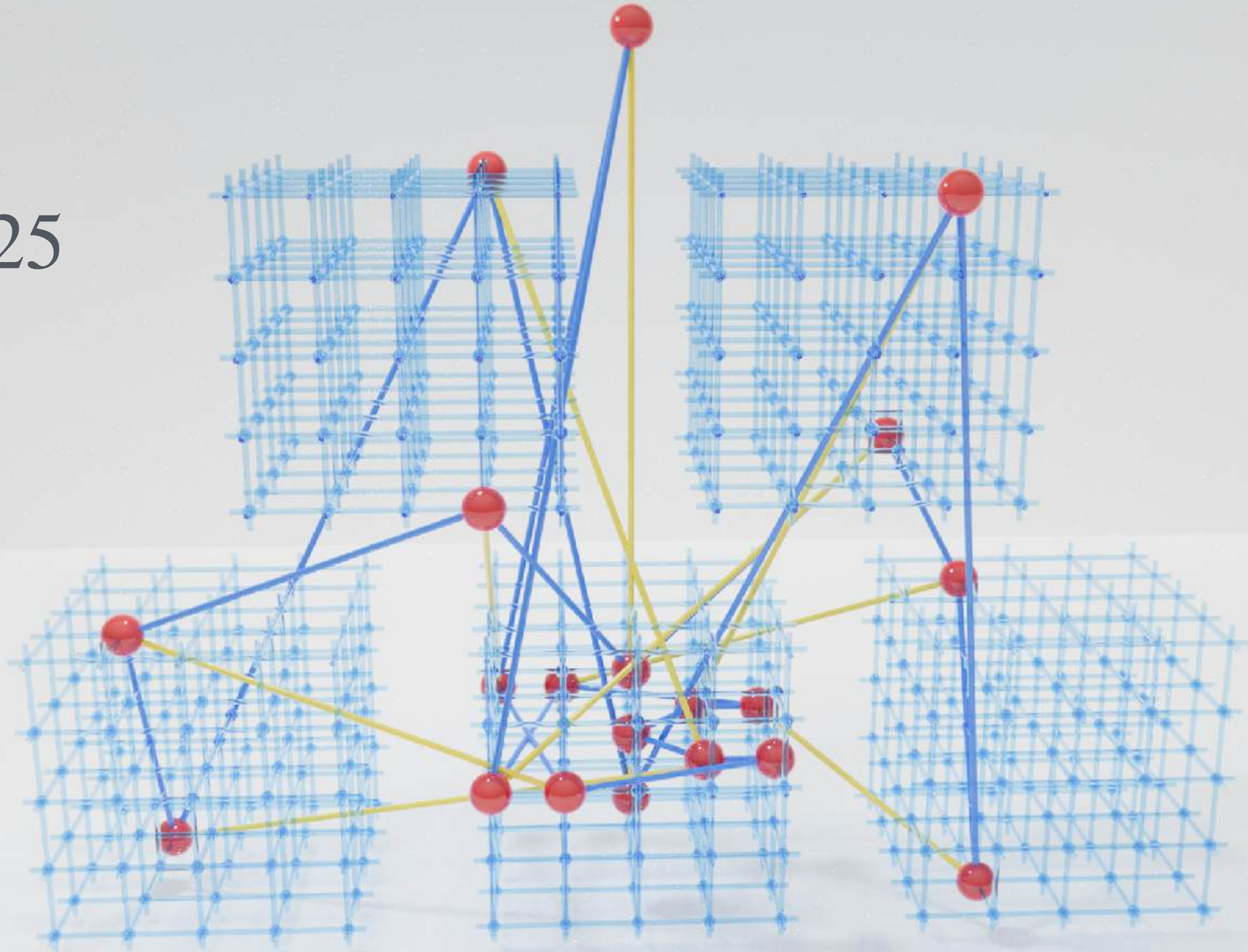
$$y^2 = x^3 + 3x \mod 5$$





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

mod 5, over $\mathbb{F}_{25}$

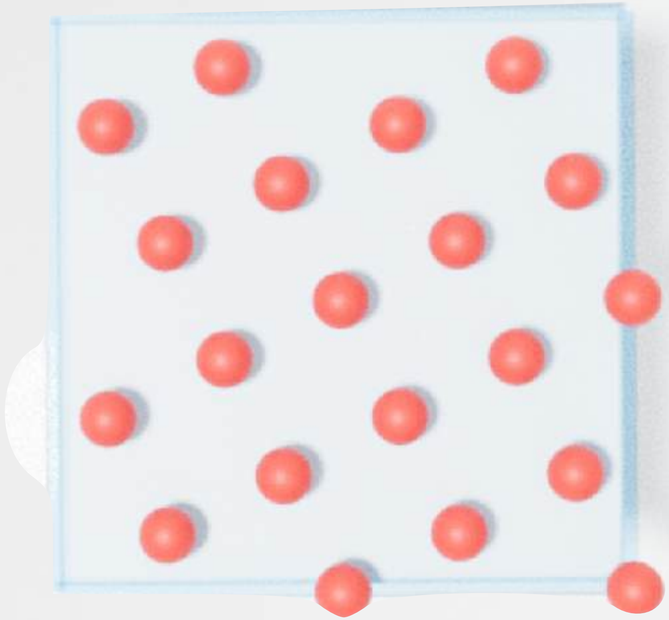


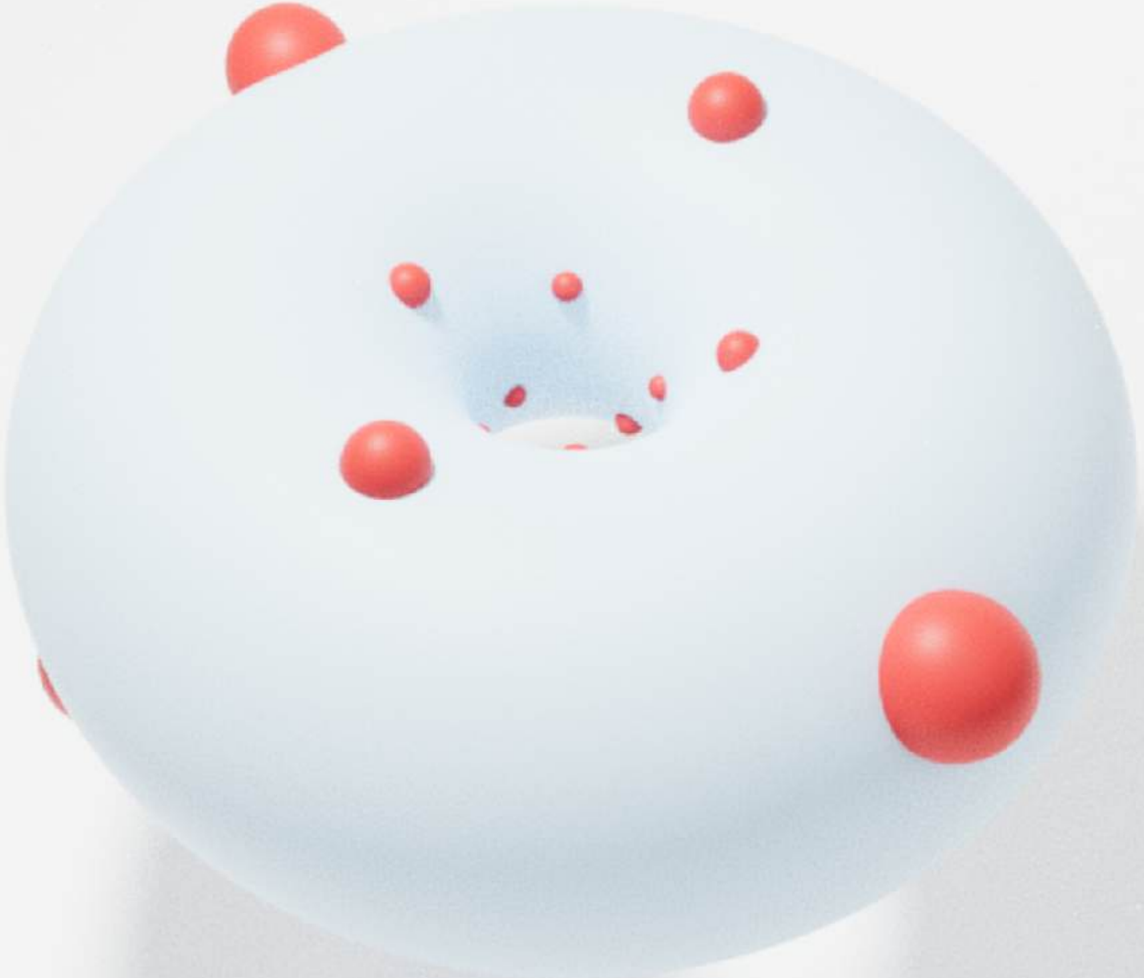
Same curve, same characteristic, lives inside the same algebraic closure

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

$$\text{mod } 5, \text{over } \mathbb{F}_{25}$$

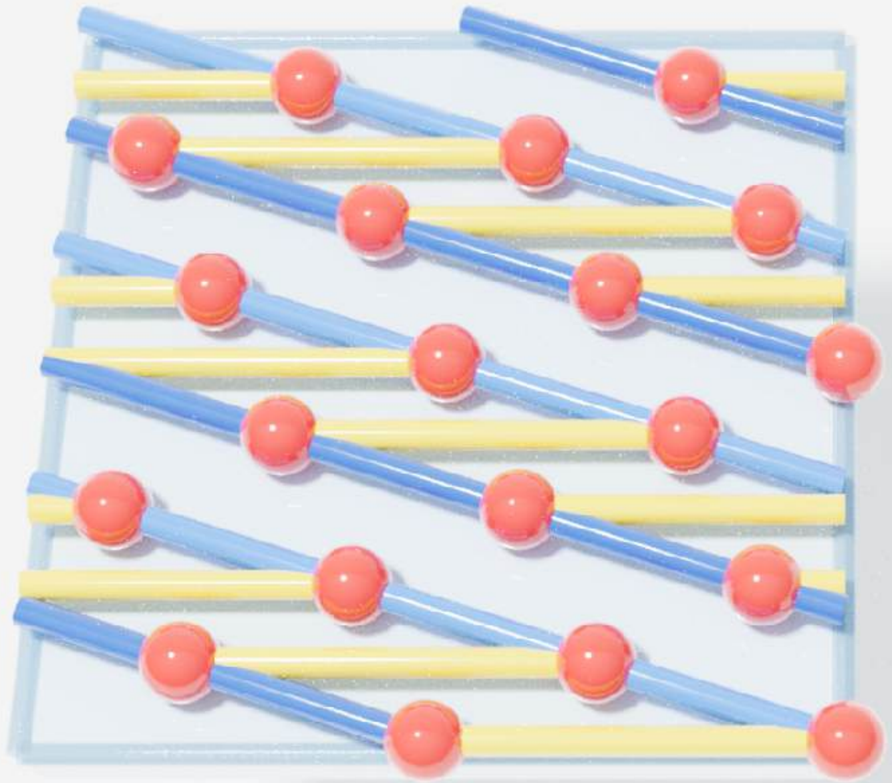
Fixed points of $z \mapsto (-2+i)^2 z$





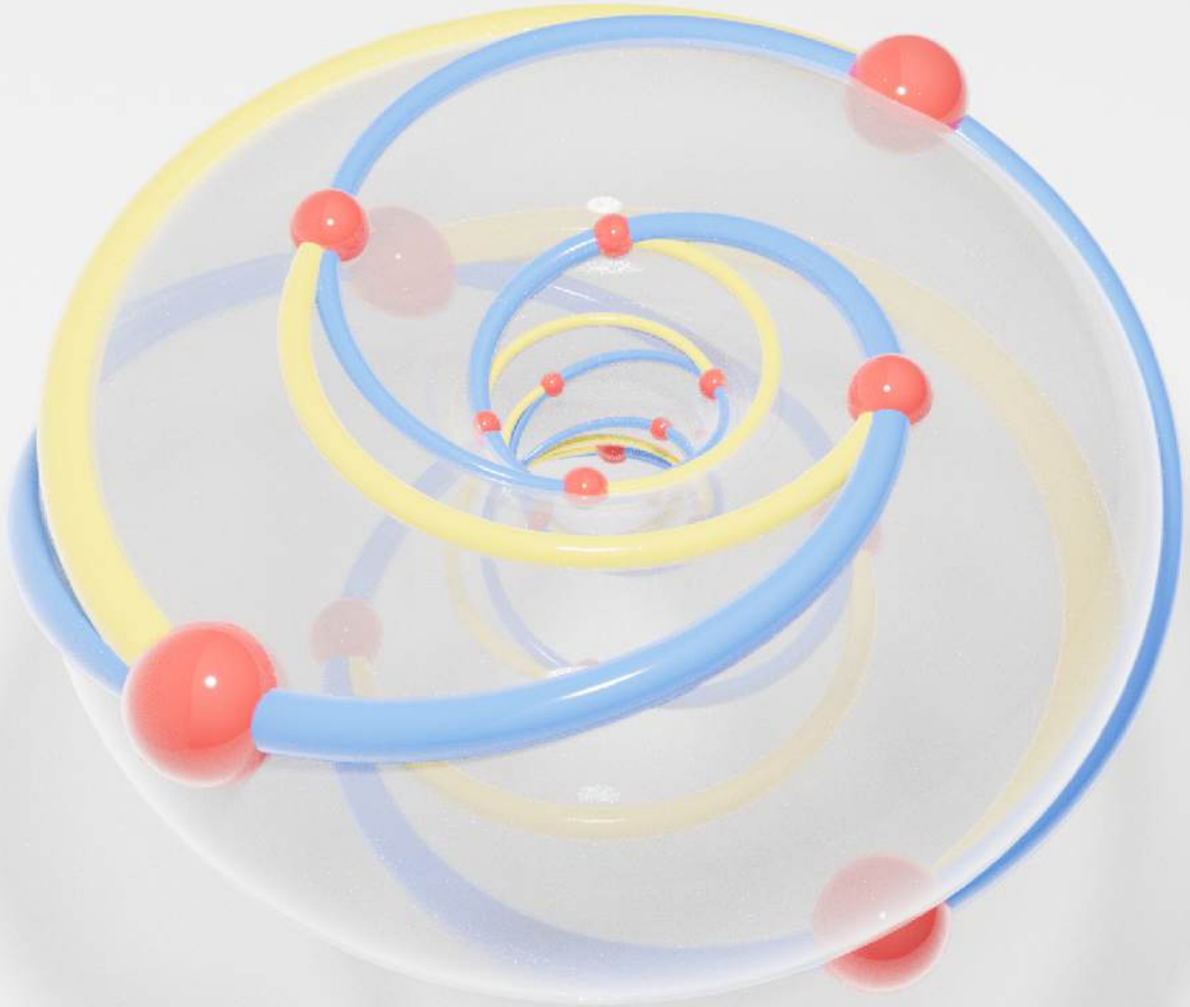
$$y^2 = x^3 + 3x$$
$$\text{mod } 5, \text{over } \mathbb{F}_{25}$$

The curve is a subgroup of the torus $\cong \mathbb{Z}_2 \times \mathbb{Z}_{10}$



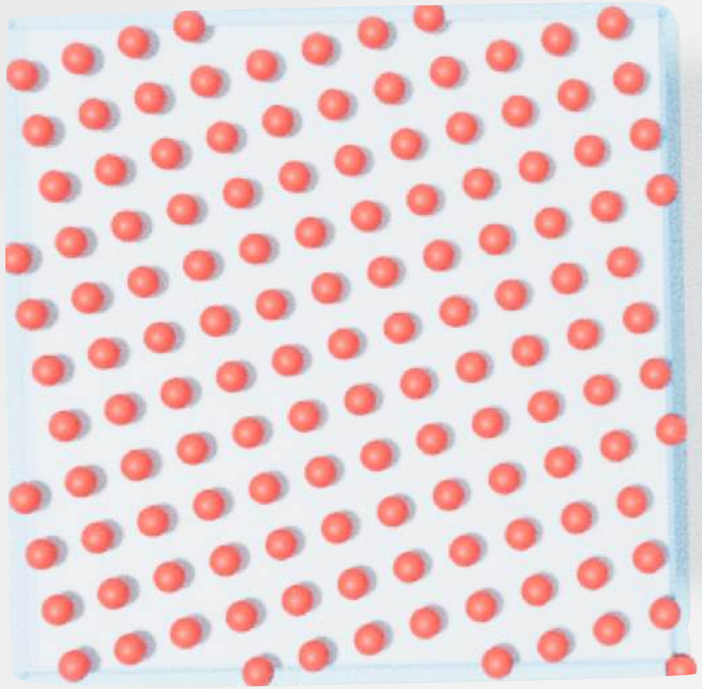
$$y^2 = x^3 + 3x$$
$$\text{mod } 5, \text{over } \mathbb{F}_{25}$$

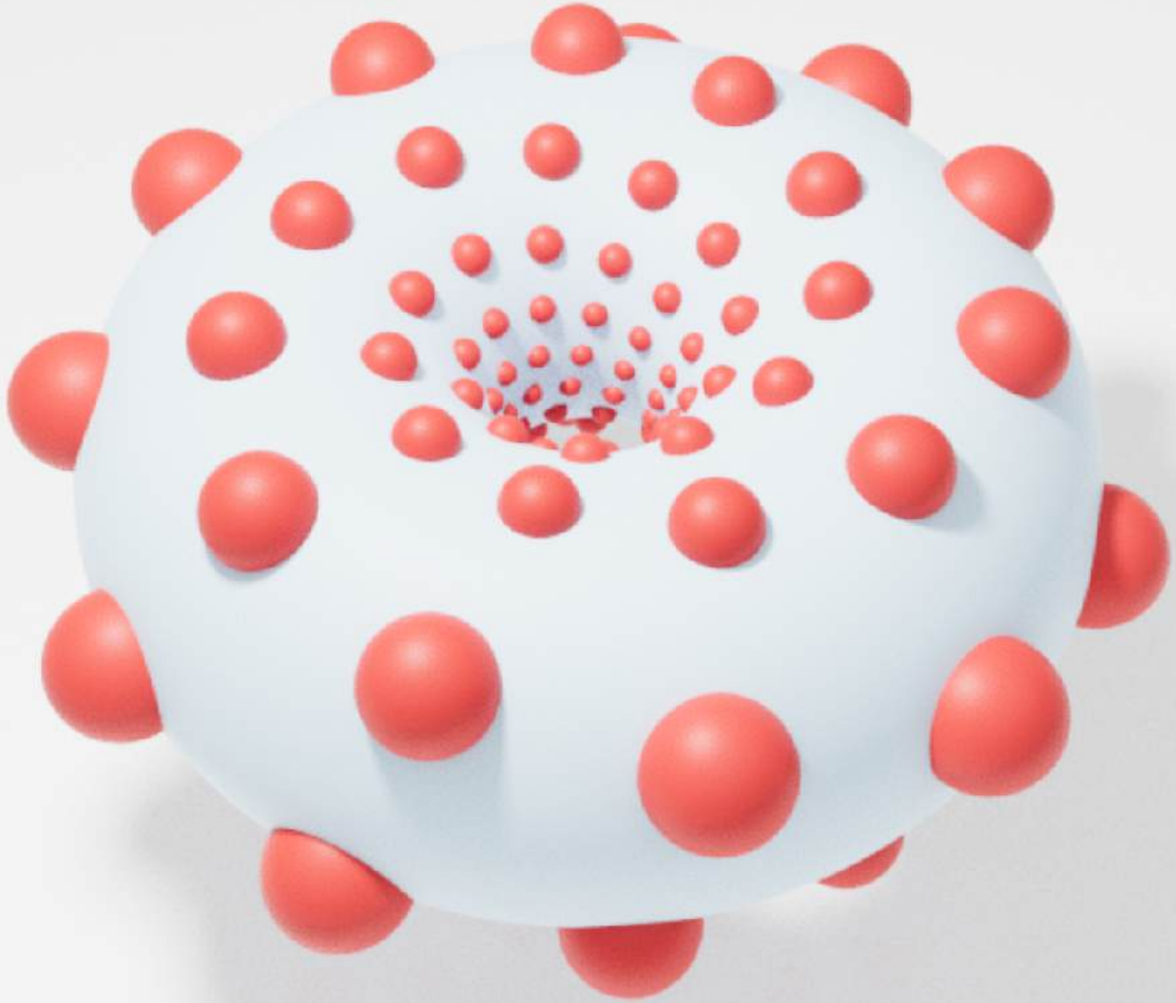
The curve is a subgroup of the torus $\cong \mathbb{Z}_2 \times \mathbb{Z}_{10}$



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

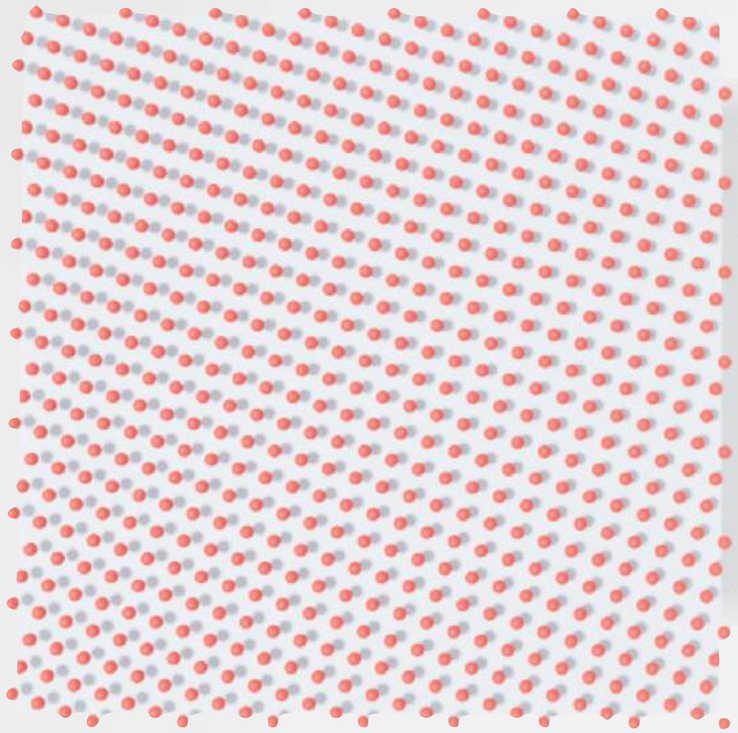
mod 5, over $\mathbb{F}_{125}$

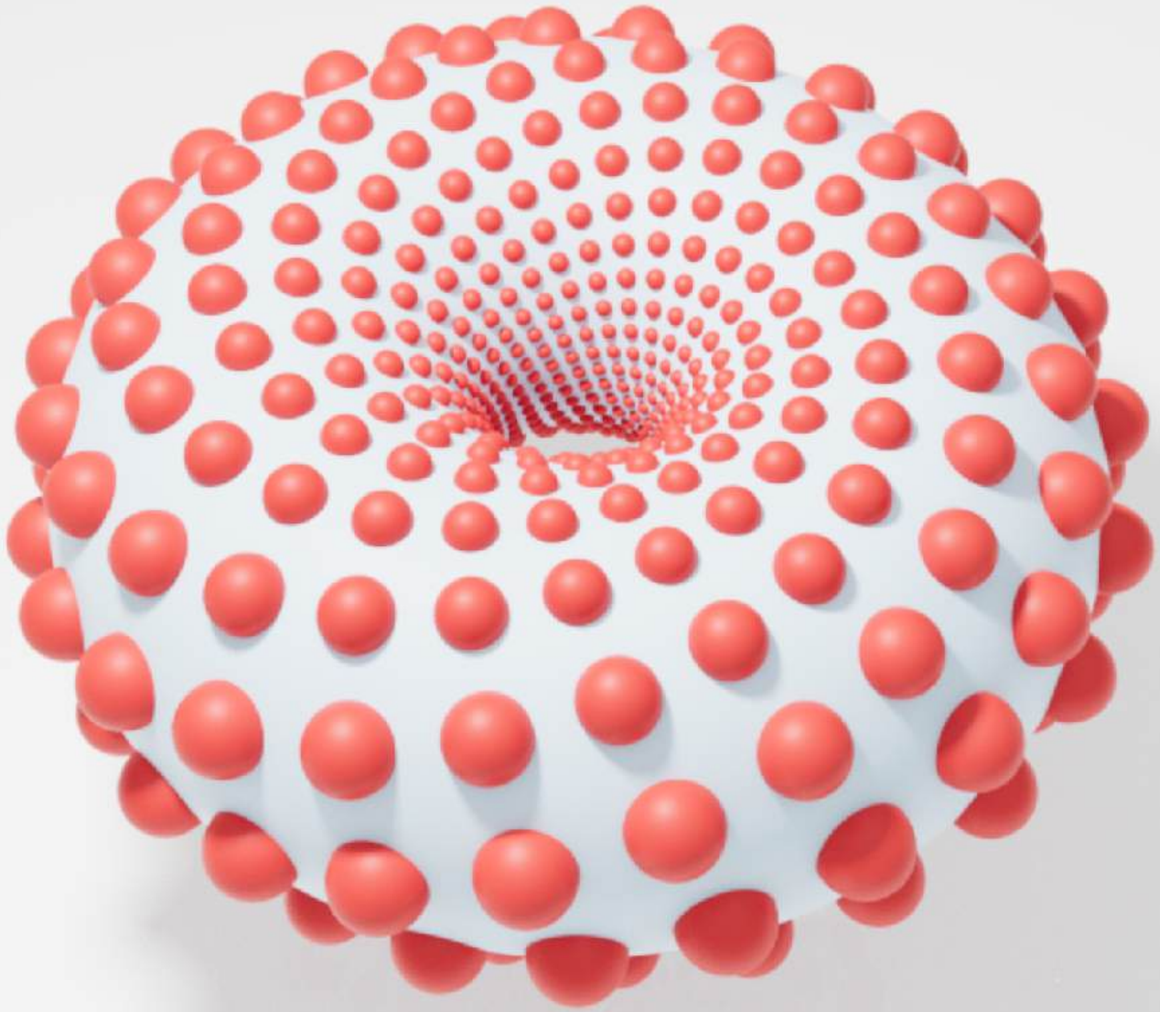




$$y^2 = x^3 + 3x$$

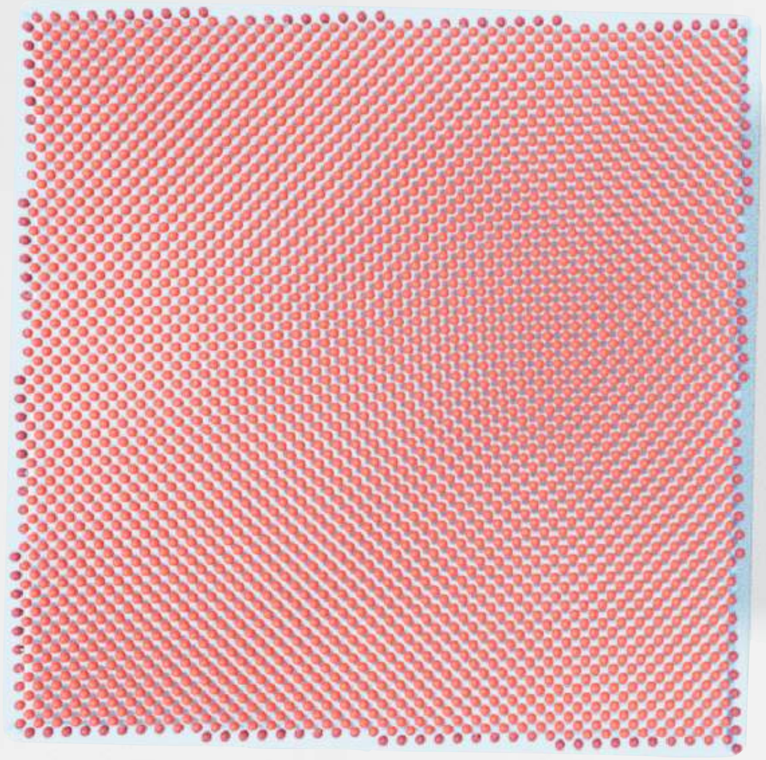
mod 5, over $\mathbb{F}_{625}$

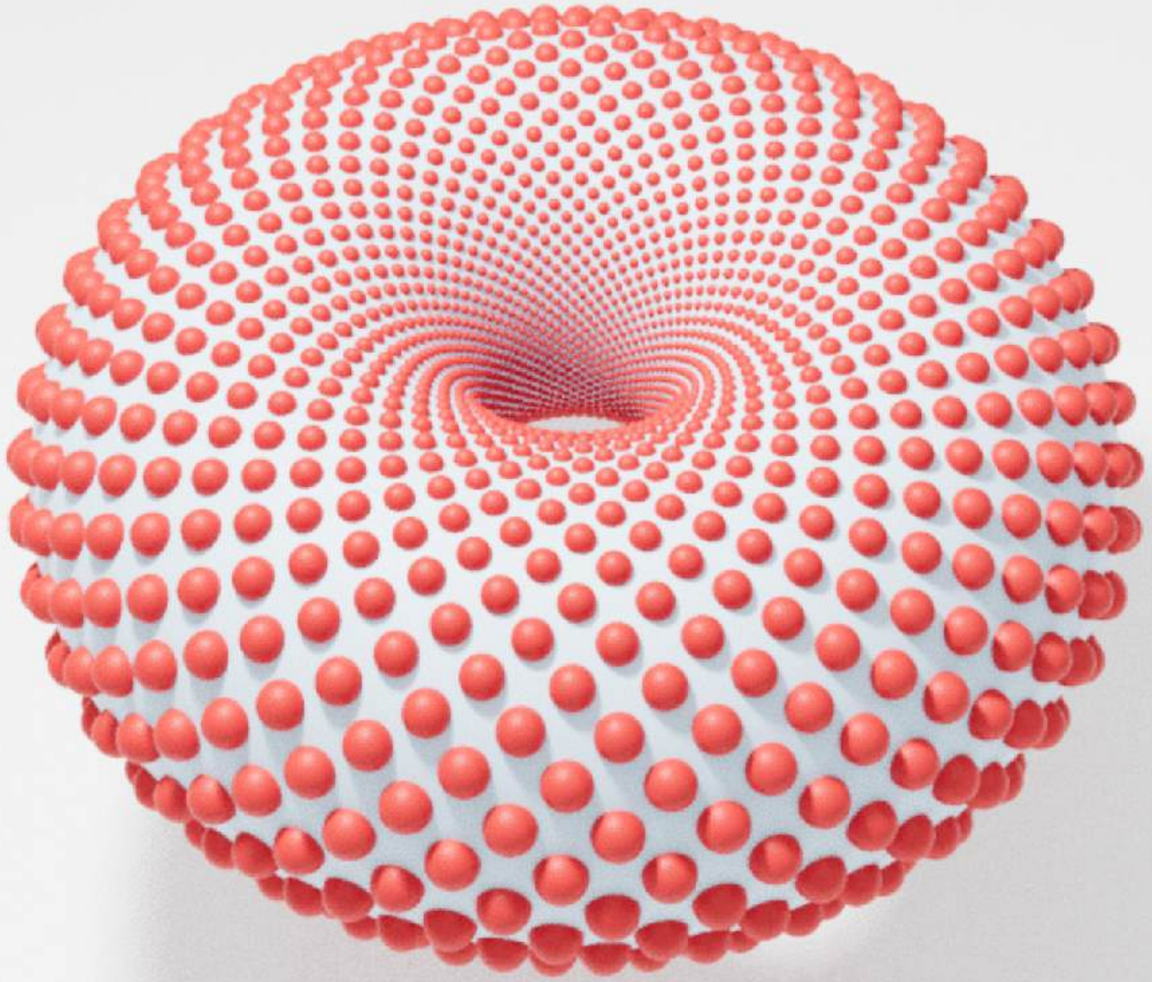




$$y^2 = x^3 + 3x$$

mod 5, over $\mathbb{F}_{3125}$

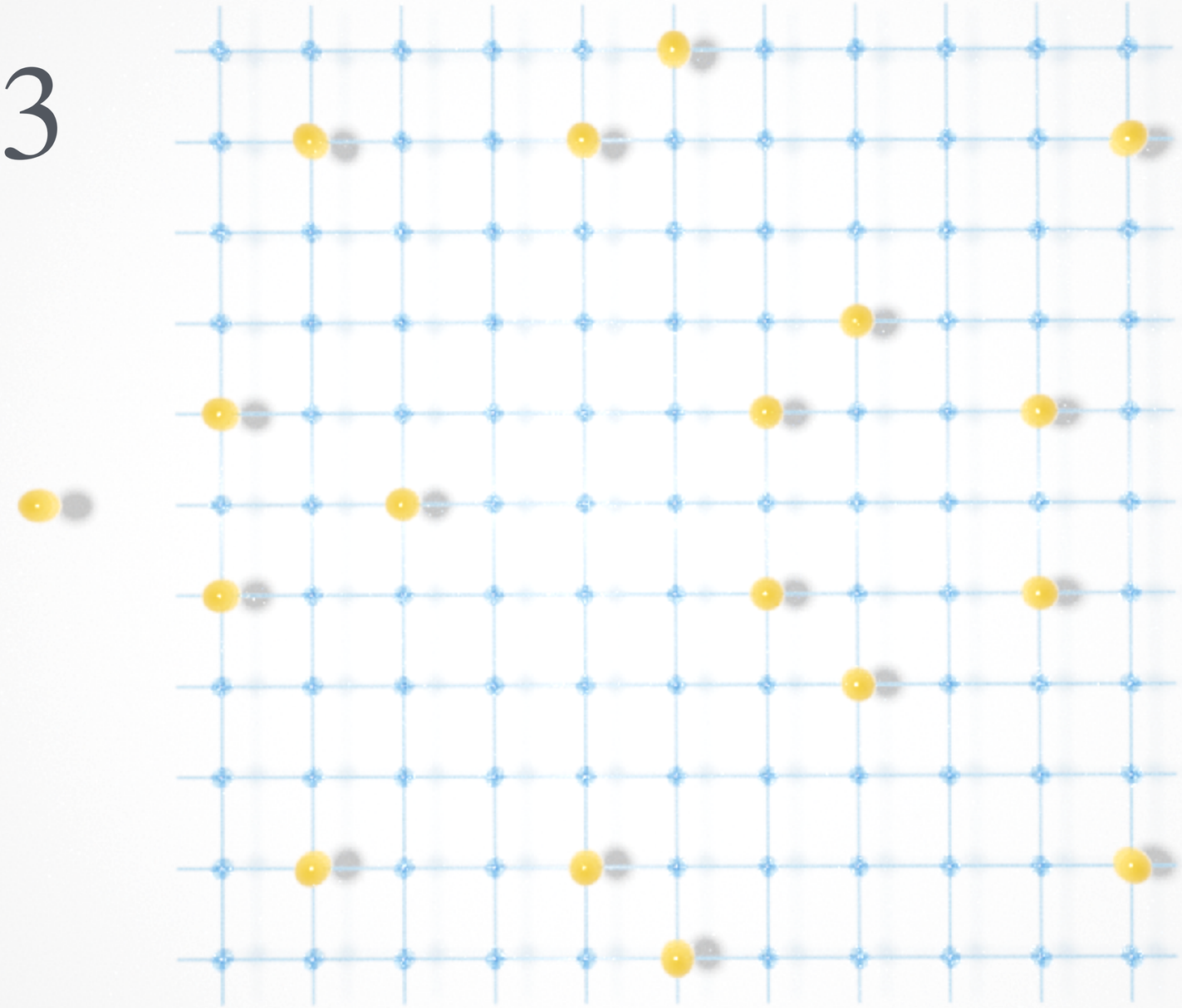




$$y^2 = x^3 + x + 3 \mod 11$$

Frobenius satisfies

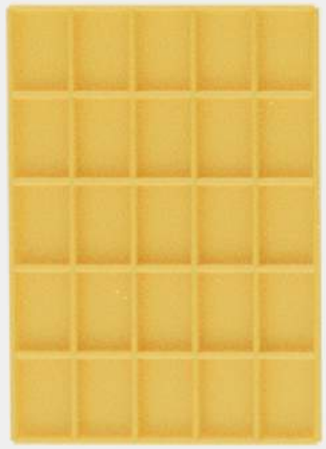
$$\phi^2 + 6\phi + 11 = 0$$



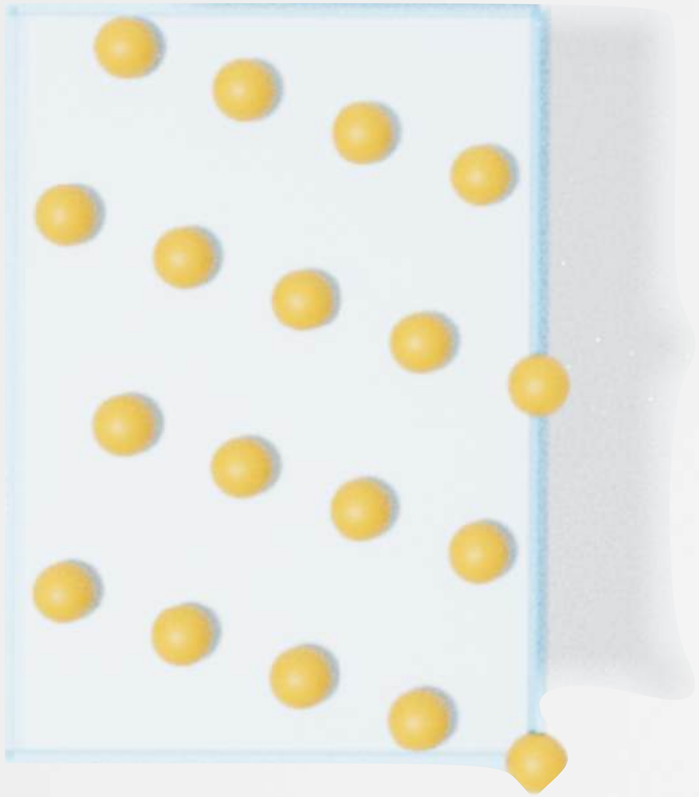
Frobenius lifts as

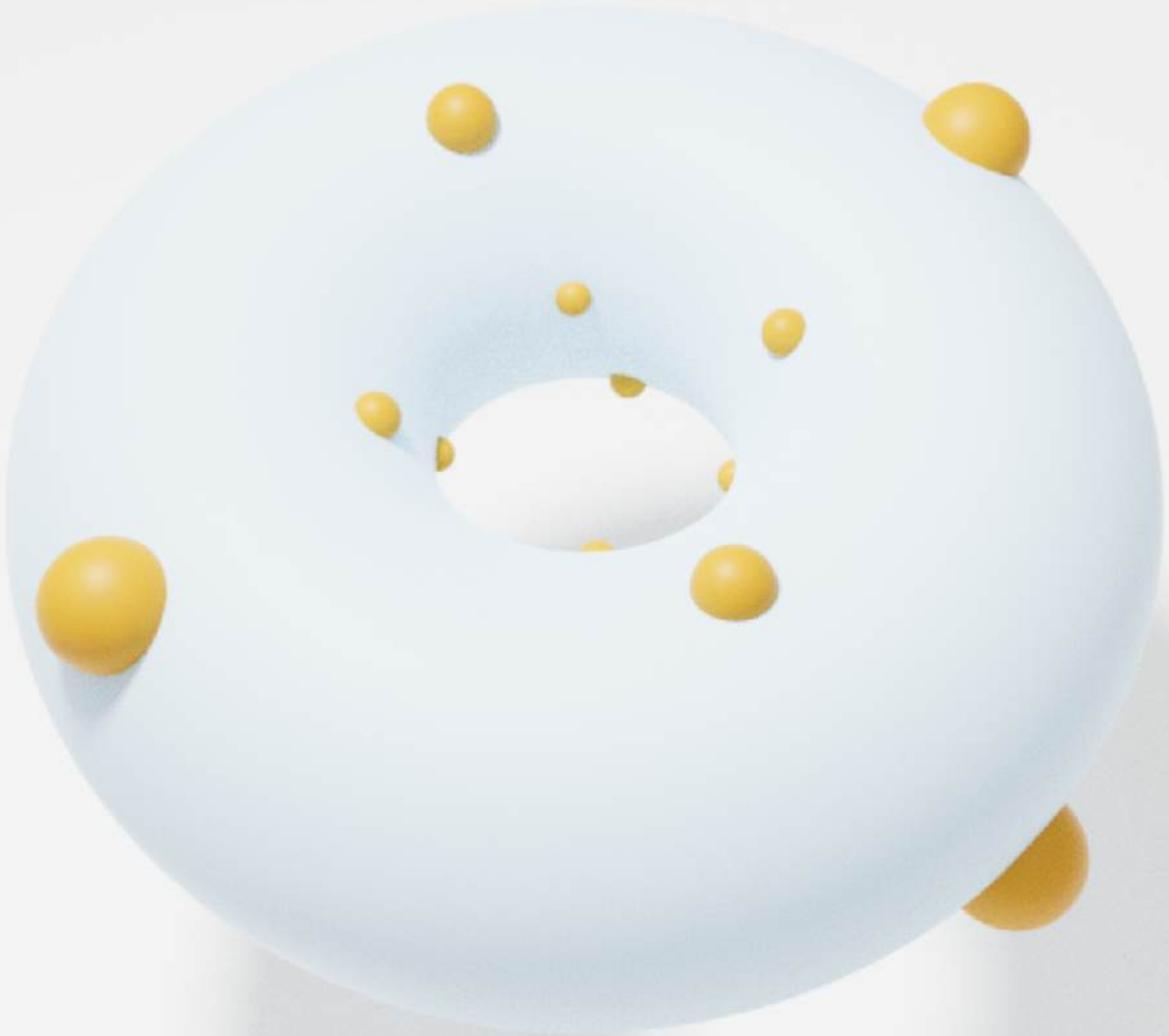
$$z \mapsto (-3 + i\sqrt{2})\, z$$

on $\mathbb{Z} \oplus i\sqrt{2}\mathbb{Z}$



$$y^2 = x^3 + x + 3 \mod 11$$





$$y^2 = x^3 + x + 3 \mod 11$$

over $\mathbb{F}_{121}$

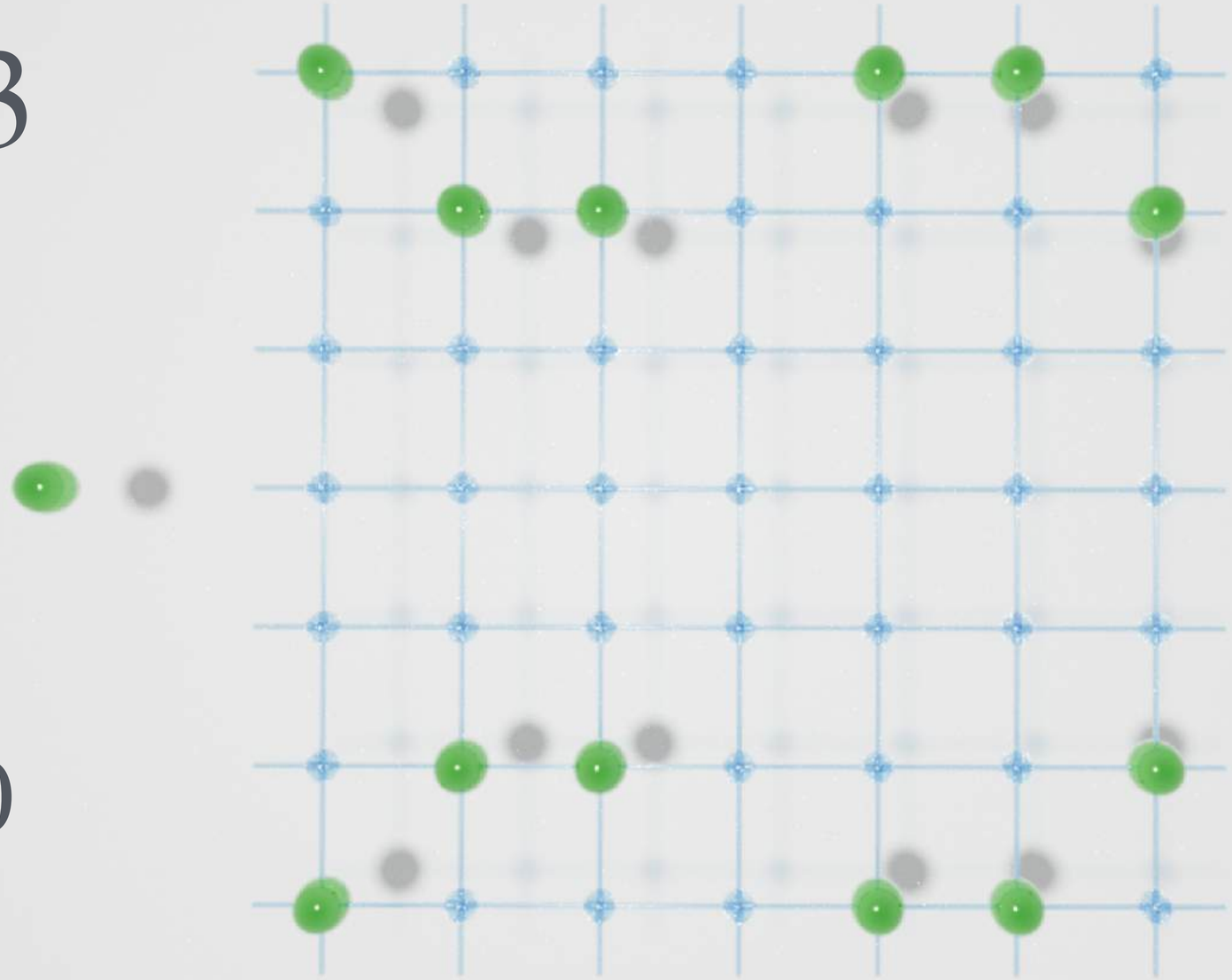
over $\mathbb{F}_{1331}$

over $\mathbb{F}_{14,641}$

$$y^2 = x^3 + 3 \mod 7$$

Frobenius satisfies

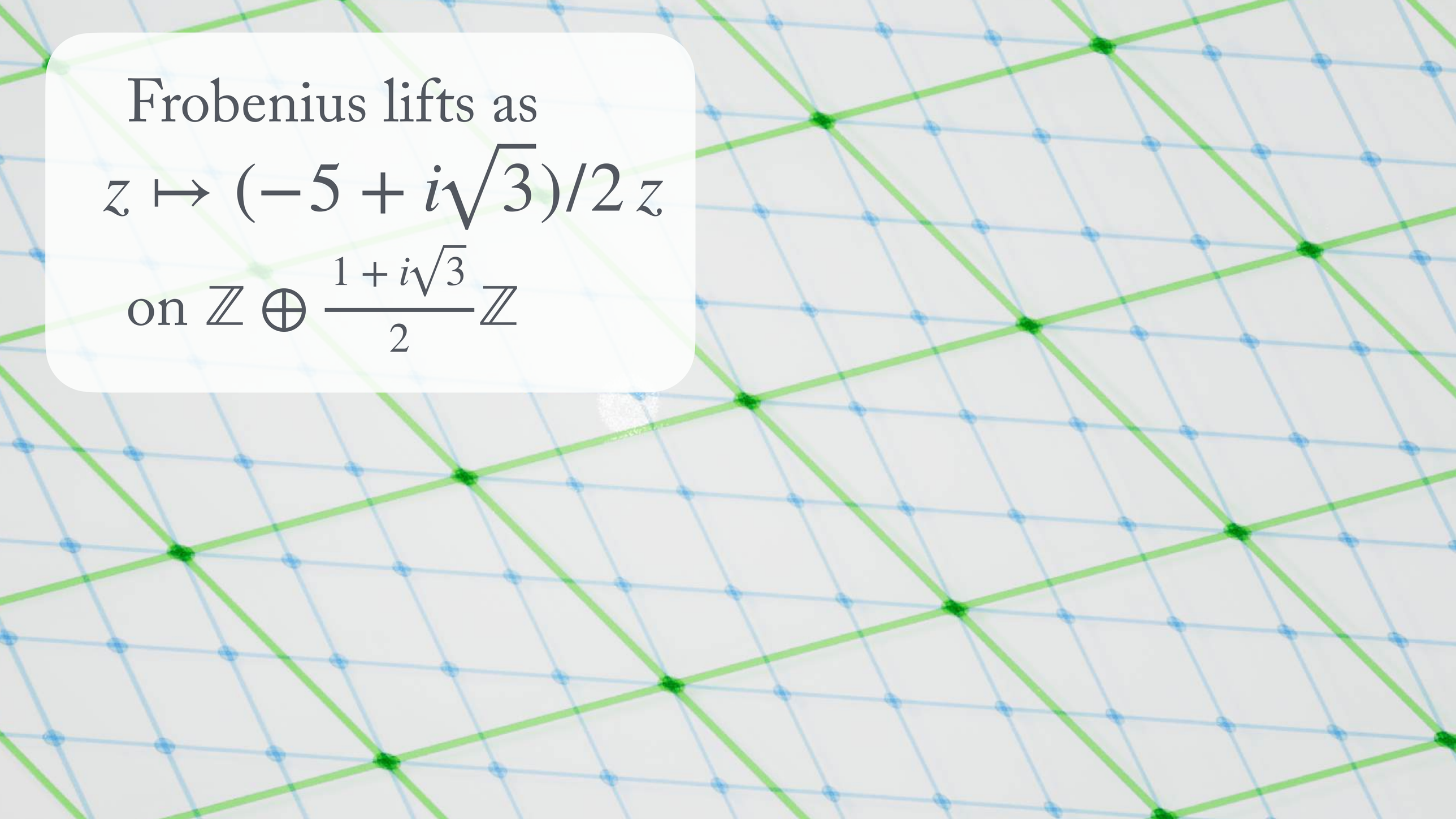
$$\phi^2 + 5\phi + 7 = 0$$



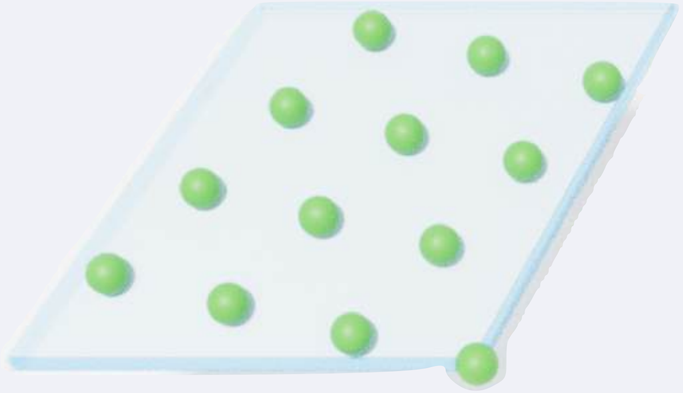
Frobenius lifts as

$$z \mapsto (-5 + i\sqrt{3})/2\, z$$

on $\mathbb{Z} \oplus \dfrac{1 + i\sqrt{3}}{2}\mathbb{Z}$

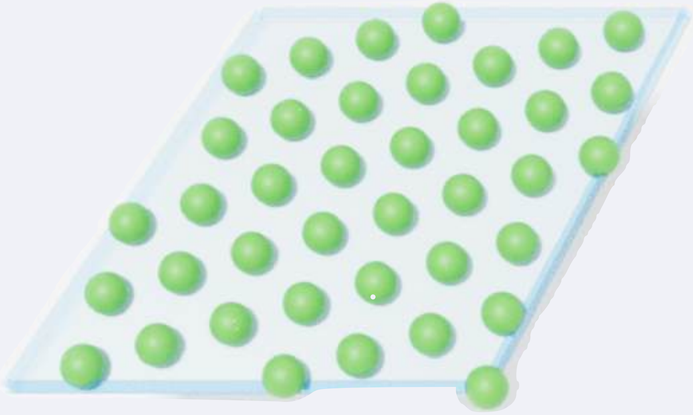


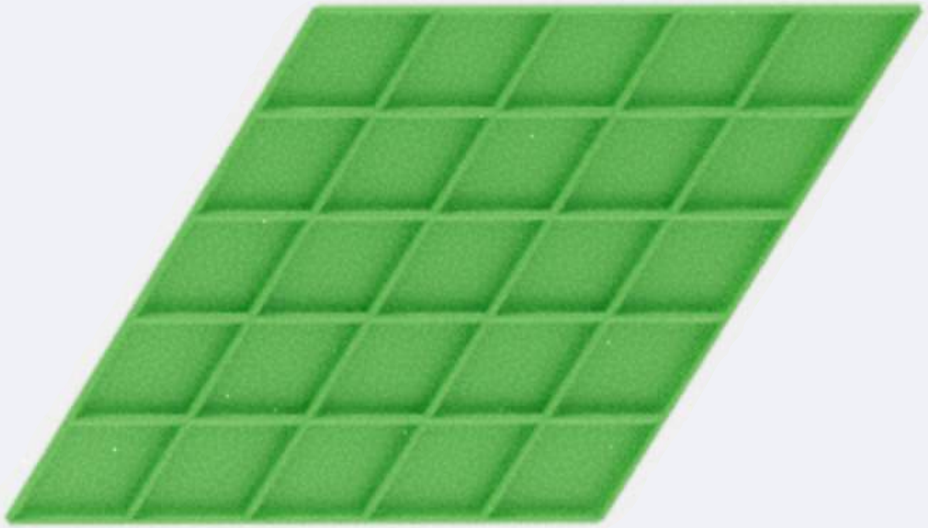
$$y^2 = x^3 + 3 \mod 7$$

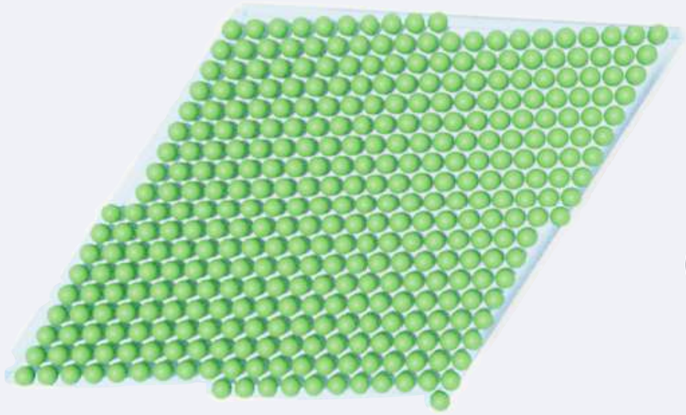


over $\mathbb{F}_7$

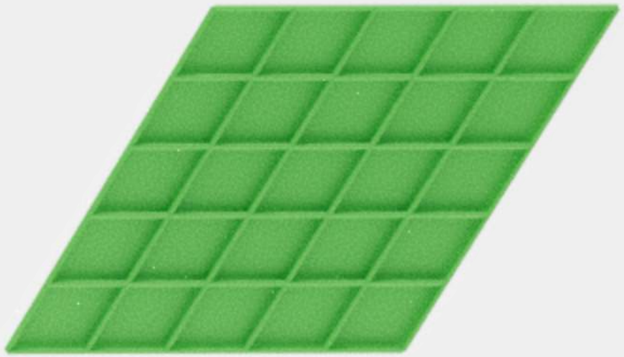
over $\mathbb{F}_{49}$

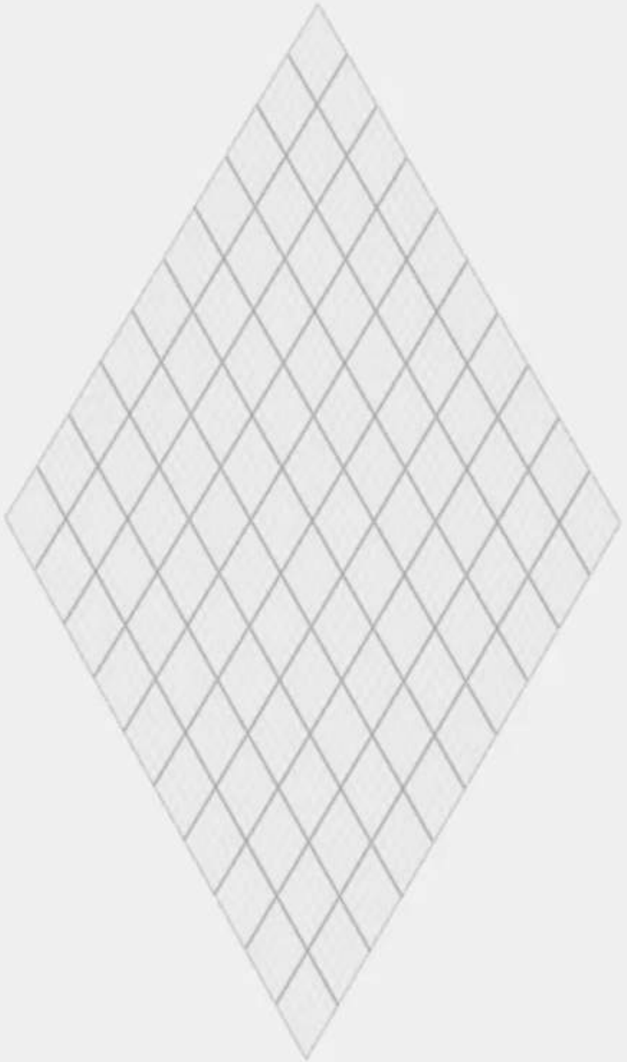




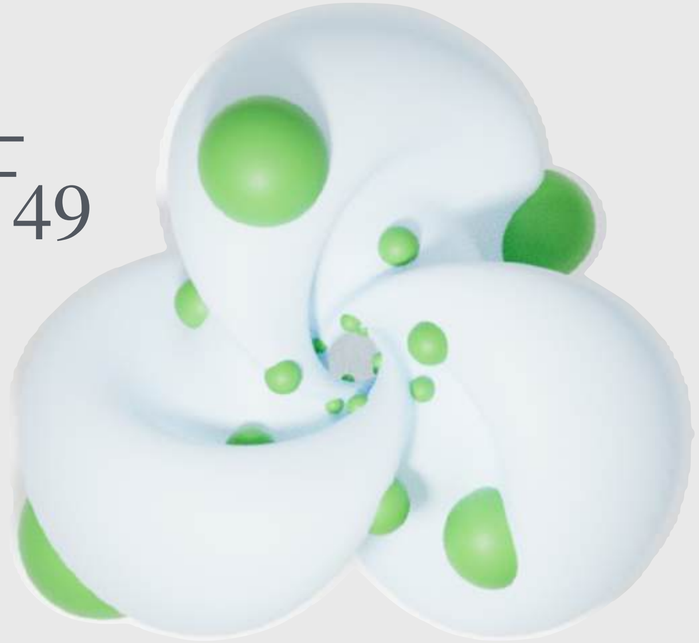


over $\mathbb{F}_{343}$

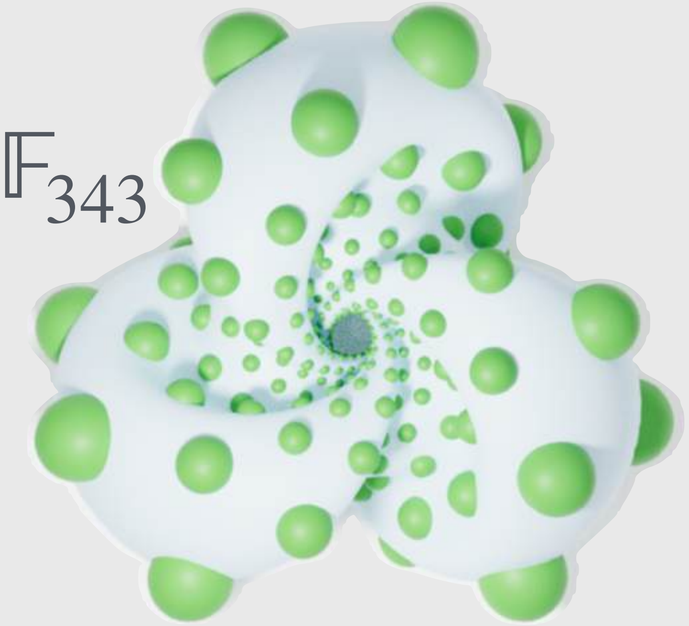




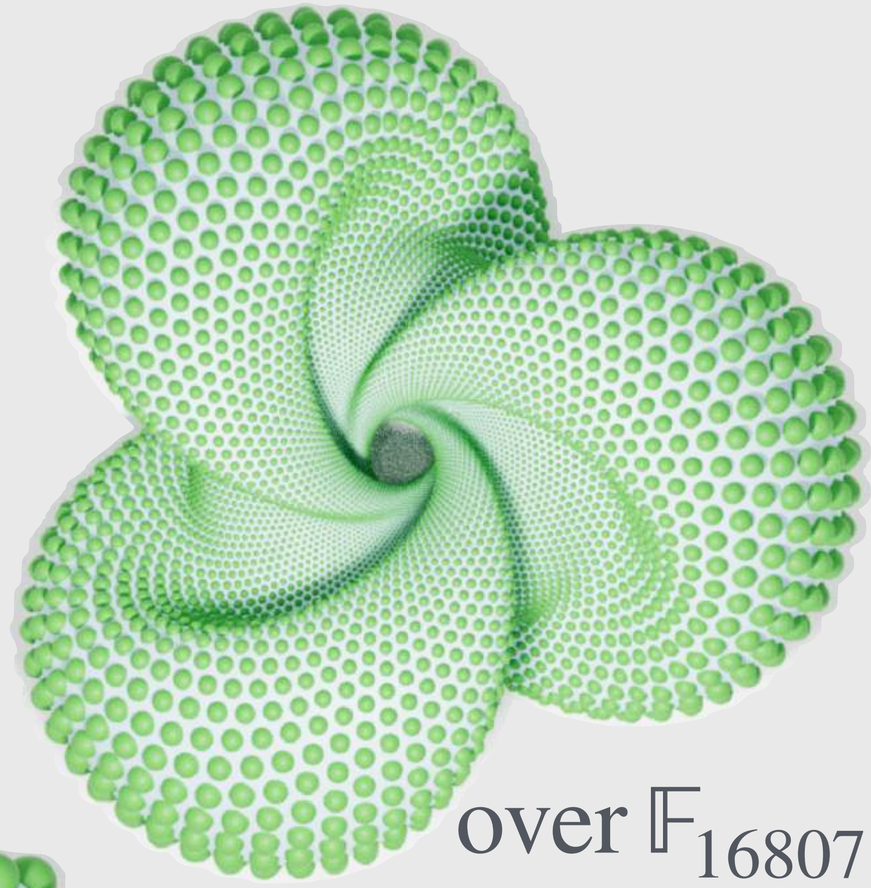
over $\mathbb{F}_{49}$



over $\mathbb{F}_{343}$



over $\mathbb{F}_{2401}$



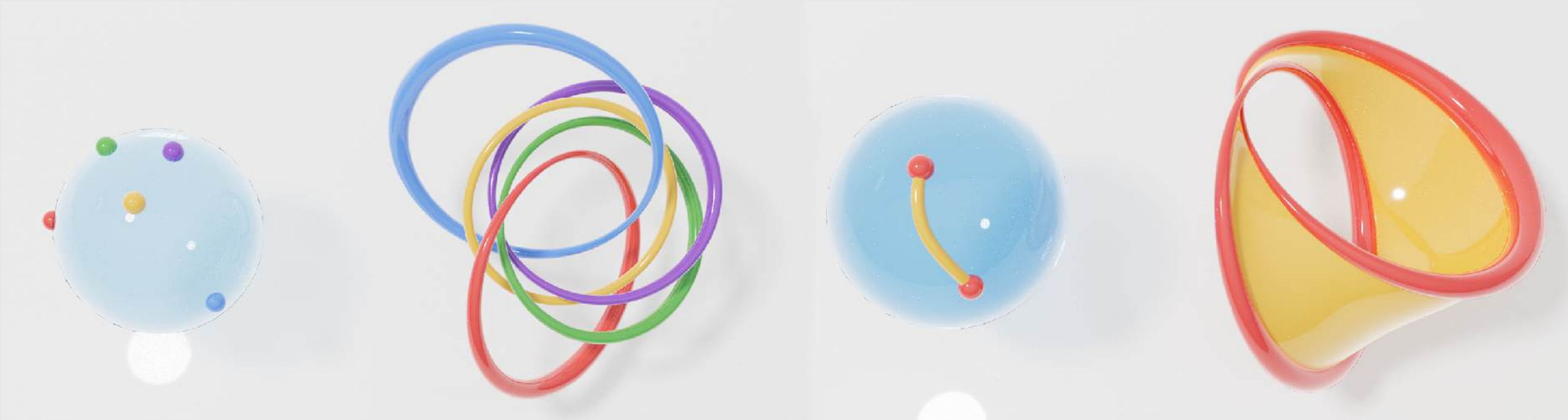
over $\mathbb{F}_{16807}$

How to roll up a torus

Geometry of the Hopf Map:

Preimages of points are circles

Preimages of curves are flat surfaces

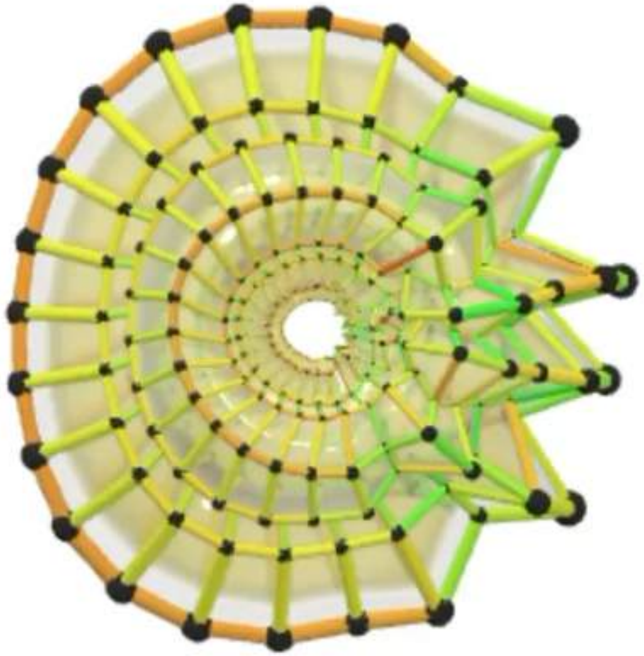


How to roll up a torus

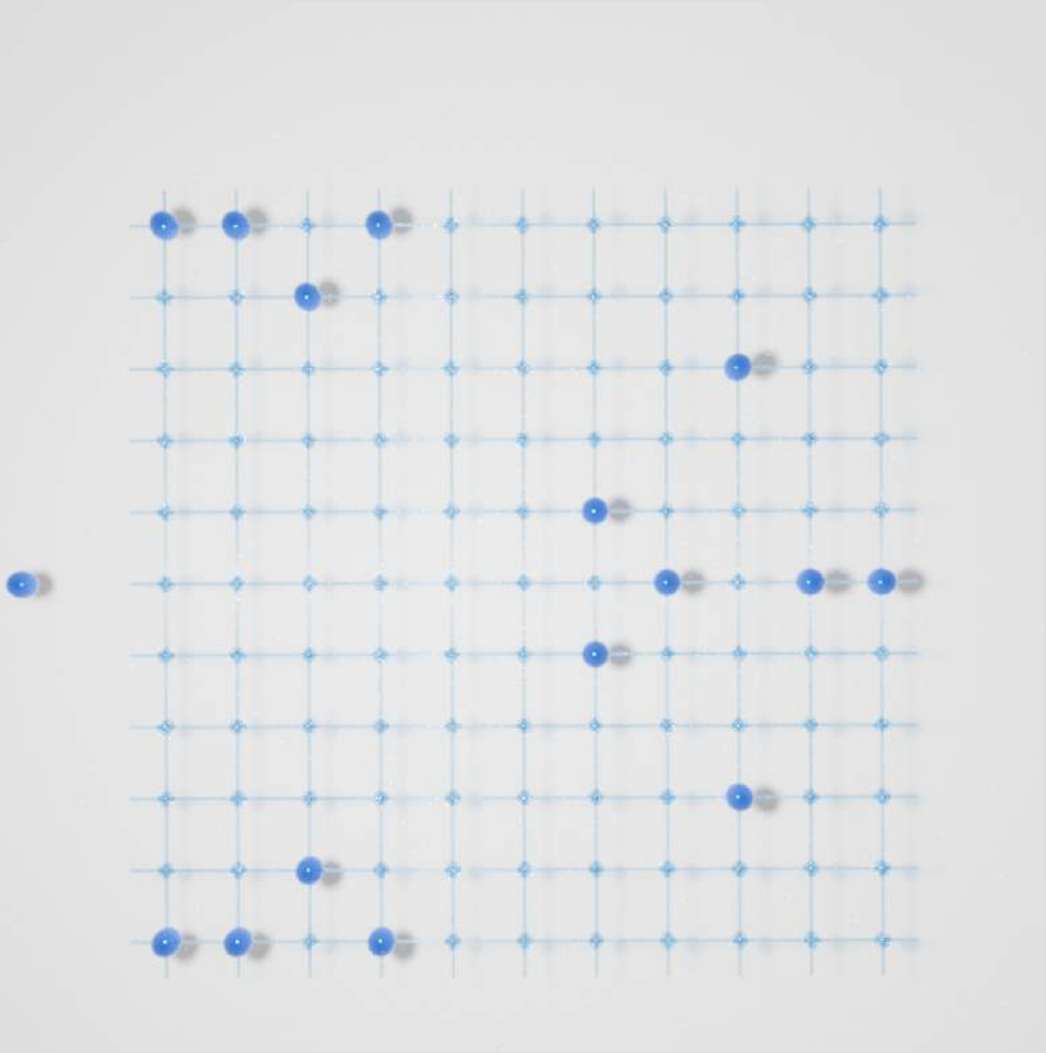
Thm (Pinkall 85)

All flat tori are preimages of closed curves under the Hopf map

Fabian Lander

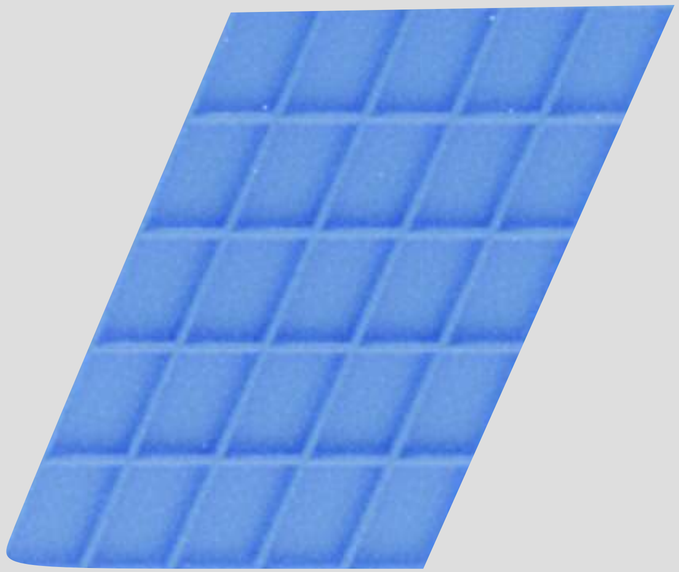


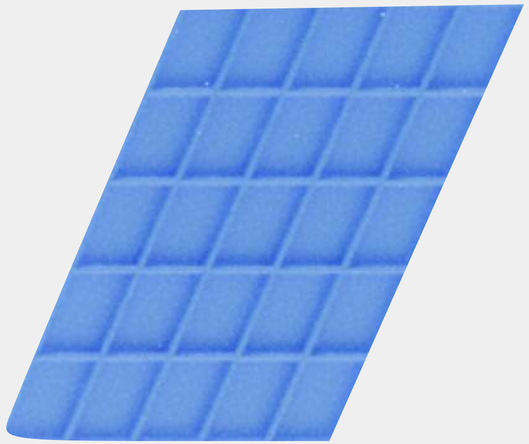
Numerically finding isometric embeddings of flat tori in $\mathbb{S}^3$ (and other surfaces in other spaces!)

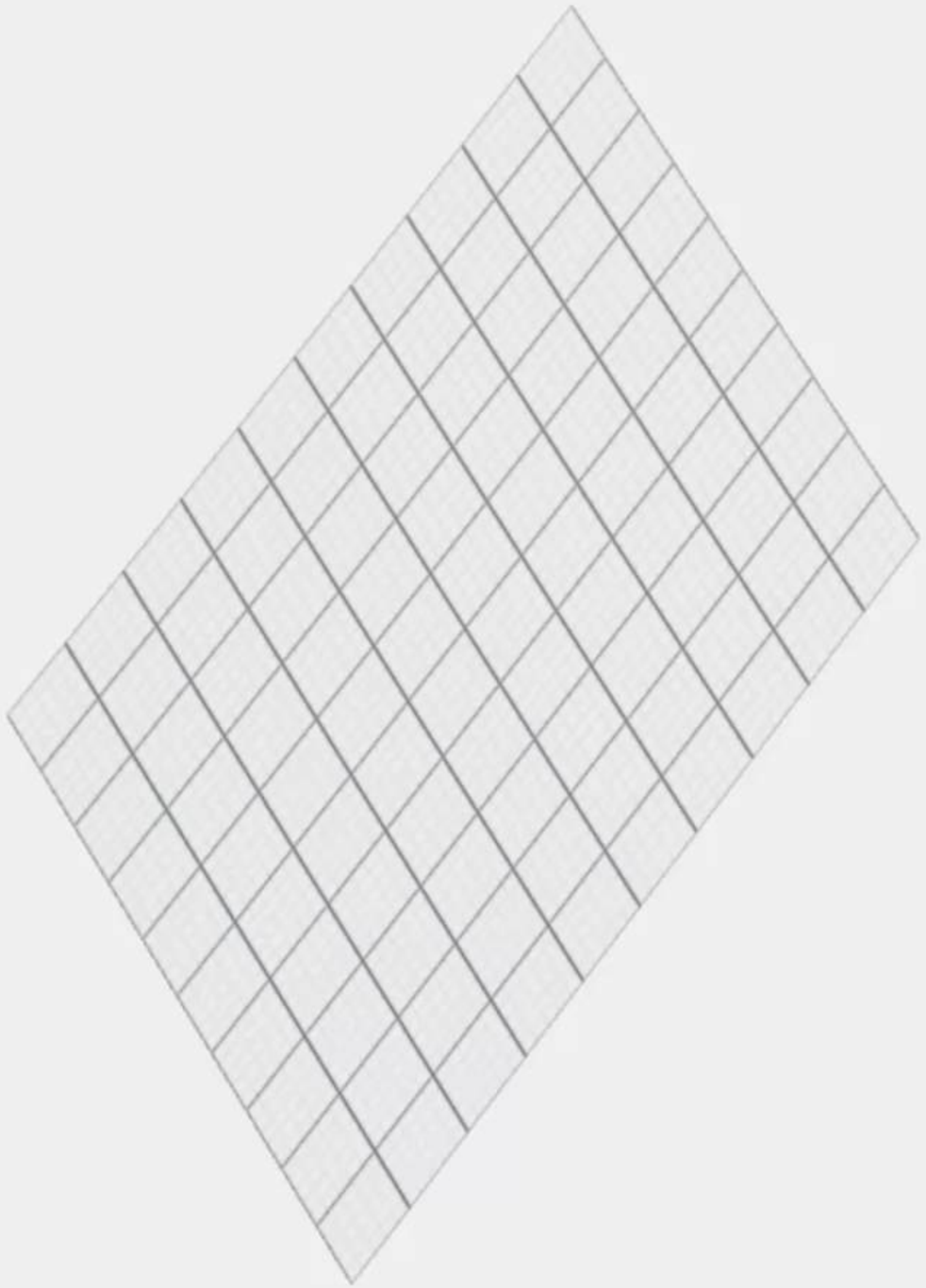


$$y^2 = x^3 + 5x + 7$$

$$\text{mod } 11$$



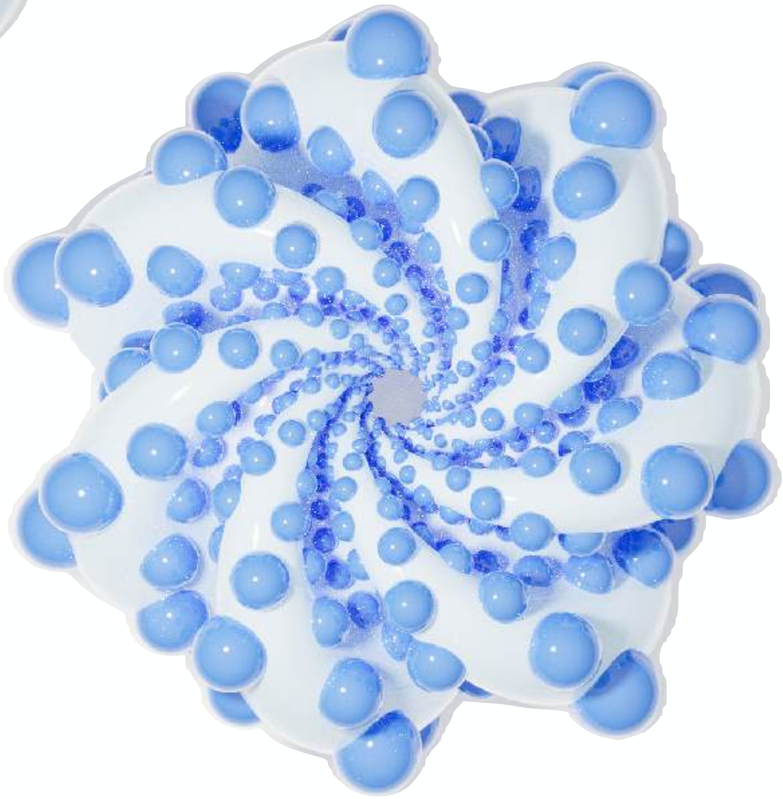


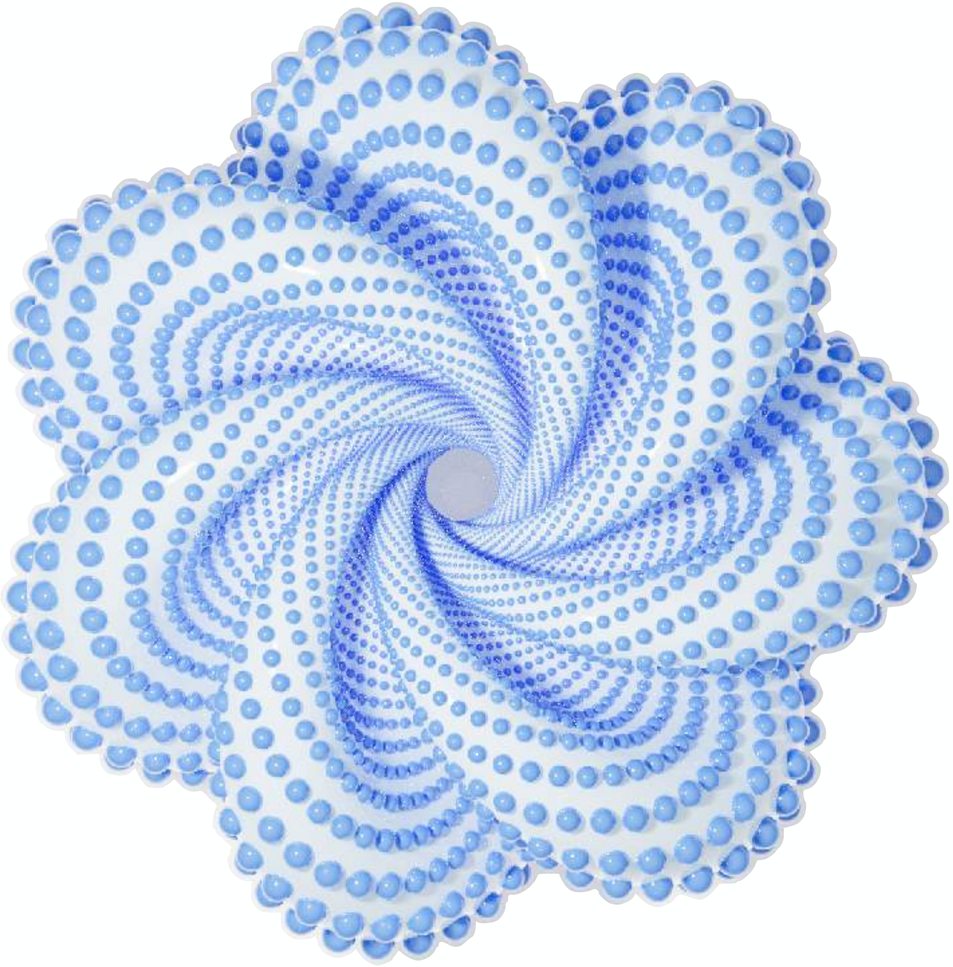


$$y^2 = x^3 + 5x + 7 \mod 11$$

over $\mathbb{F}_{49}$

over $\mathbb{F}_{49}$

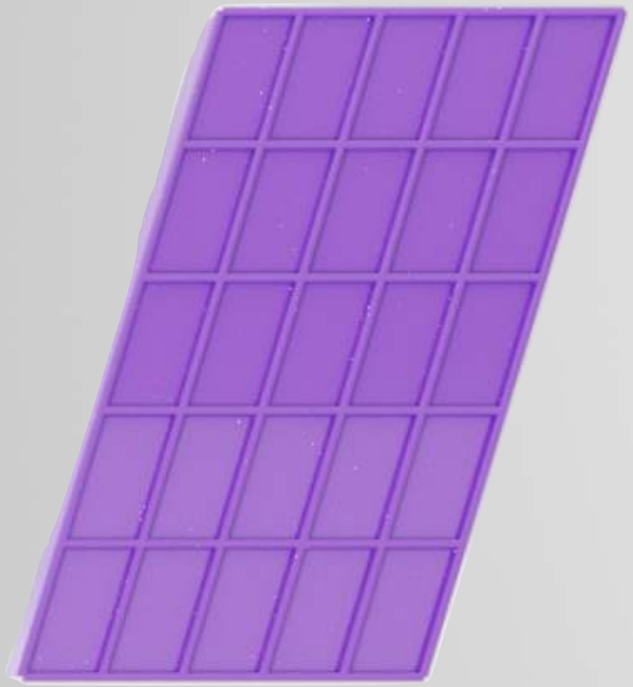


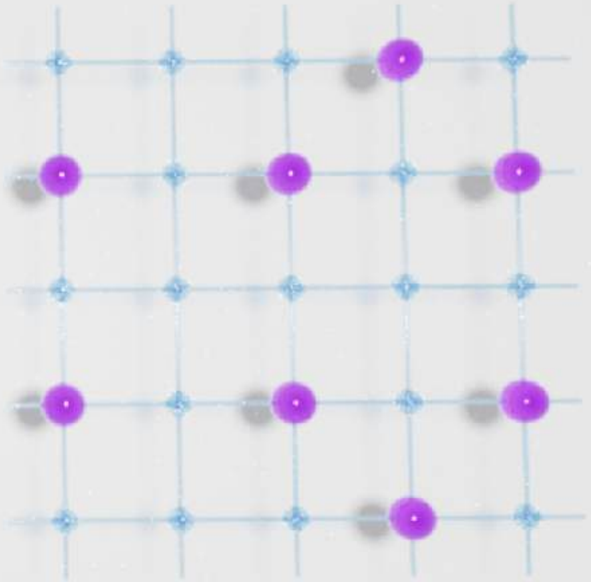


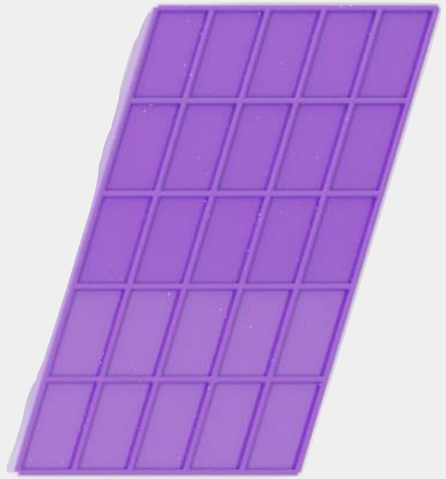
over $\mathbb{F}_{49}$

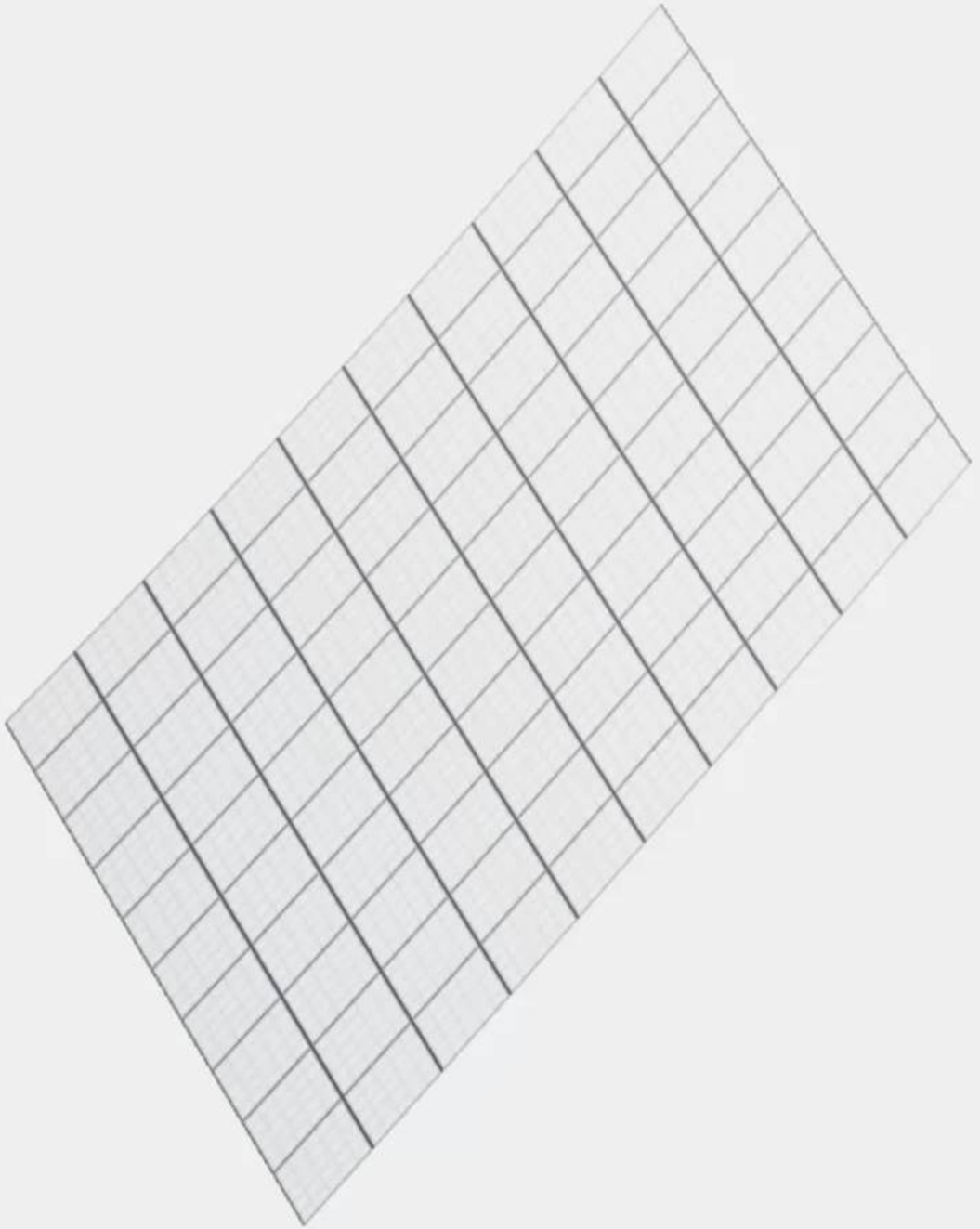
$$y^2 = x^3 + x + 1$$

$$\text{mod } 5$$



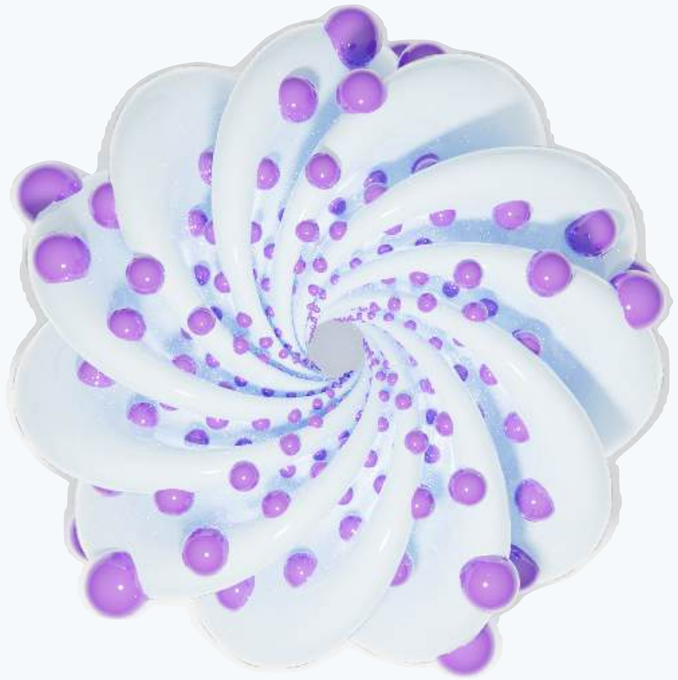






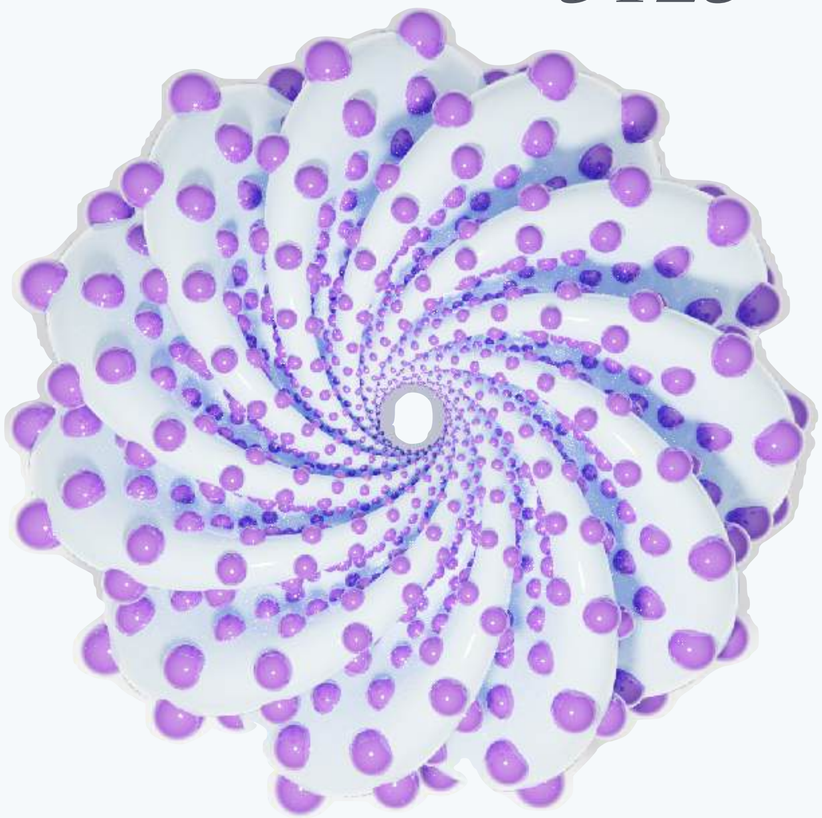
$$y^2 = x^3 + x + 1 \mod 5$$

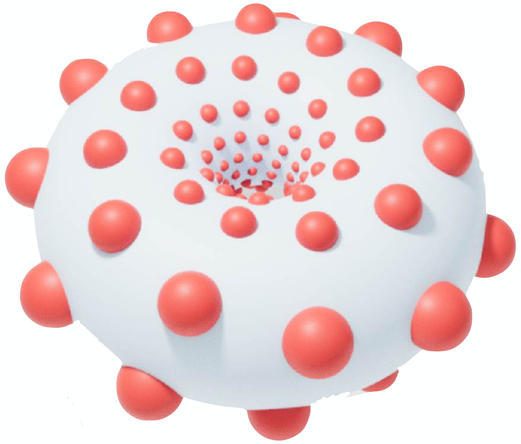
over $\mathbb{F}_{125}$



over $\mathbb{F}_{625}$

over $\mathbb{F}_{3125}$





THANKS!