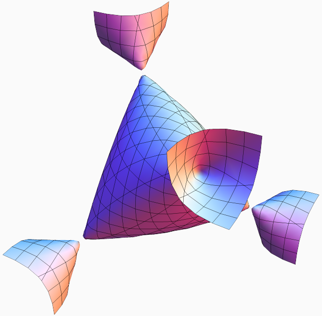
POLYNOMIALS IN THE VARIABLE p

Bailey Whitbread
AMSI Summer School 2024
The University of Queensland



Consider the circle

$$E\colon x^2 + y^2 = 1.$$

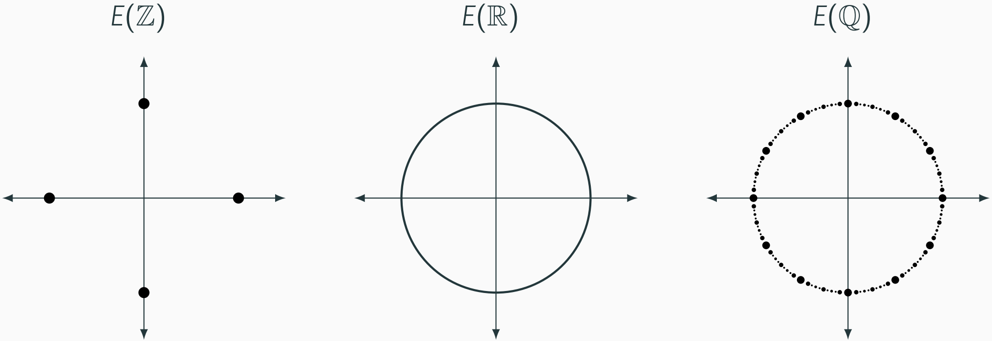
The first and last definition in this talk:

$$E(\mathbf{Set}) := \{(x, y) \in \mathbf{Set} \times \mathbf{Set} \text{ with } x^2 + y^2 = 1\}.$$

For example,

$$E(\mathbb{Z}) = \{(1, 0), (0, 1), (-1, 0), (0, -1)\}.$$

$$E\colon x^2 + y^2 = 1.$$



These are all shadows of the circle.

A special shadow

For each prime p, there is exactly one field with p elements.

$$\mathbb{F}_2,\ \mathbb{F}_3,\ \mathbb{F}_5,\ \mathbb{F}_7,\ \mathbb{F}_{11},\ \mathbb{F}_{13},\ \mathbb{F}_{17},\ \mathbb{F}_{19},\ \ldots$$

In particular,

$$\mathbb{F}_2 = \{0, 1\}$$

$$\mathbb{F}_3 = \{0, 1, 2\}$$

$$\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$$

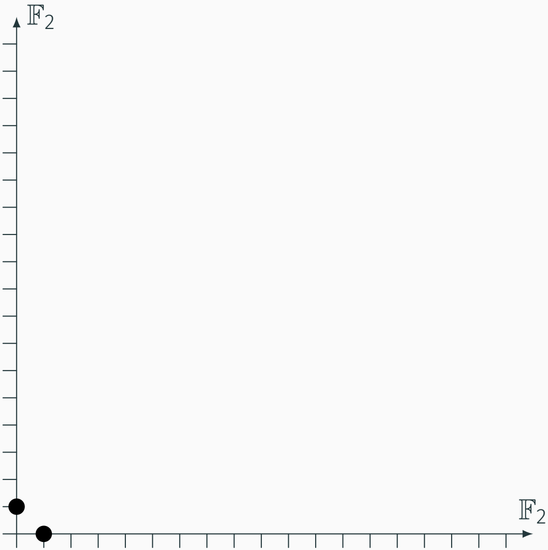
$$\vdots$$

Moral: Understand $|E(\mathbb{F}_p)| \rightsquigarrow$ Understand E

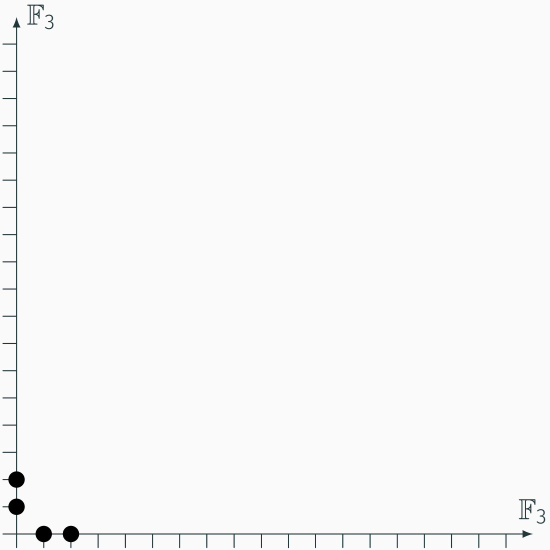
Theorem: If $|E(\mathbb{F}_p)|$ is a polynomial in p then this polynomial encodes topological info

The circle mod $p = 2$

$$E\colon x^2 + y^2 = 1$$

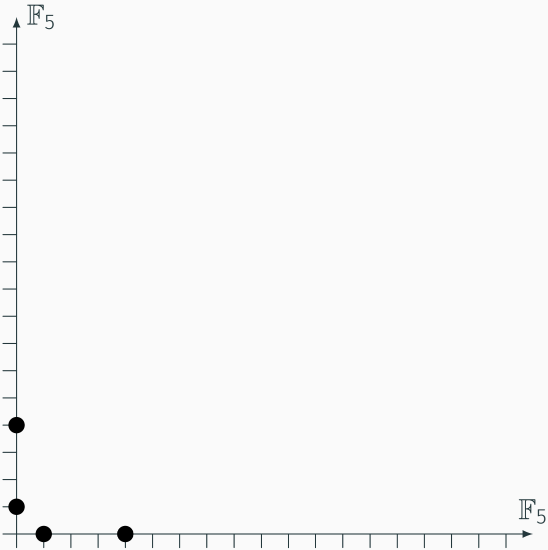


$$E\colon x^2 + y^2 = 1$$

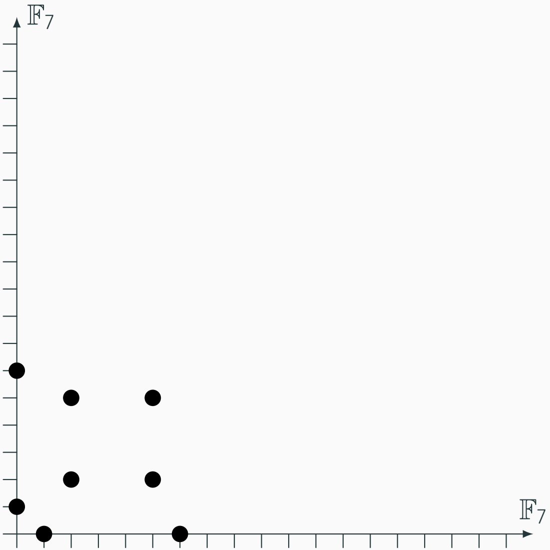


The circle mod $p = 5$

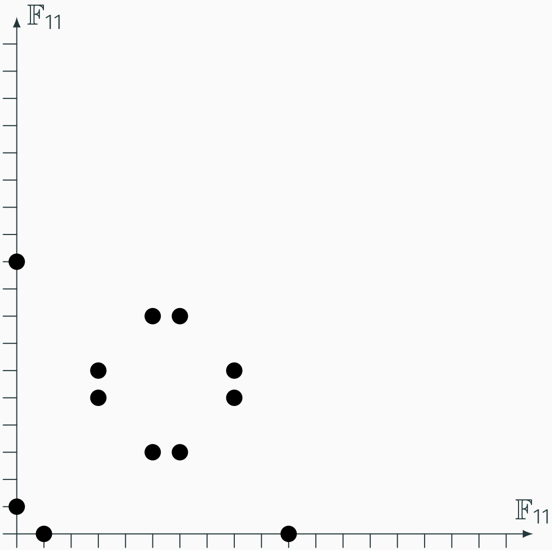
$$E\colon x^2 + y^2 = 1$$



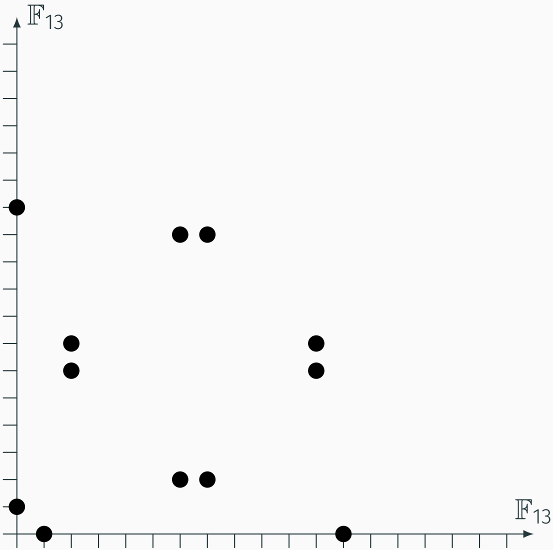
$$E\colon x^2 + y^2 = 1$$



$$E\colon x^2 + y^2 = 1$$

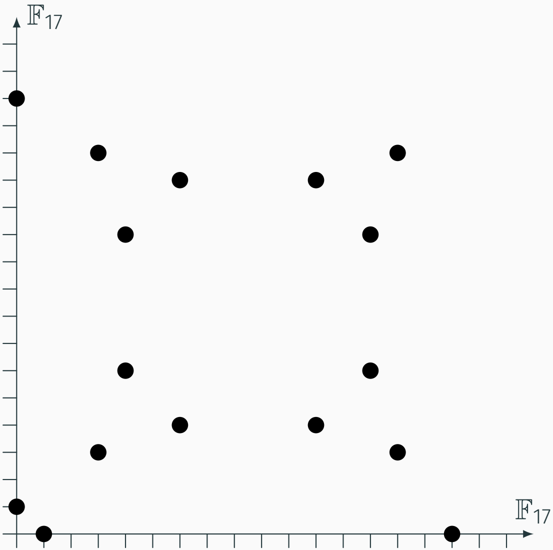


$$E\colon x^2 + y^2 = 1$$



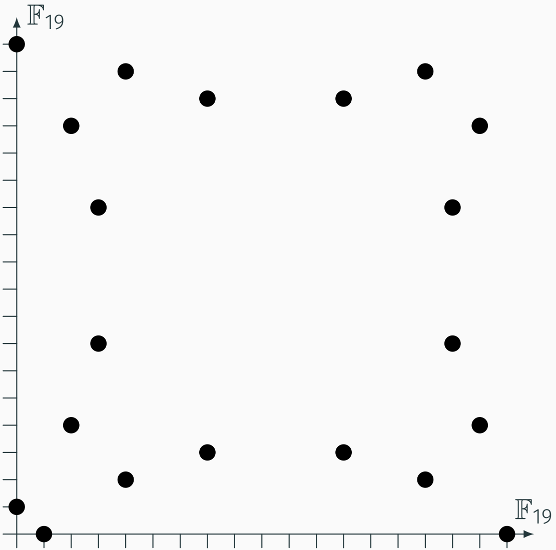
The circle mod $p = 17$

$$E\colon x^2 + y^2 = 1$$



The circle mod $p = 19$

$$E\colon x^2 + y^2 = 1$$



In general,

$$|E(\mathbb{F}_p)| \text{ “}=\text{” } p - 1.$$

How do we read this polynomial?

$$\text{dimension of } E = \deg |E(\mathbb{F}_p)| = 1$$

$$\text{\# of components of } E = \text{leading coeff. of } |E(\mathbb{F}_p)| = 1$$

$$\text{Euler characteristic of } E = |E(\mathbb{F}_p)|\Big|_{p \mapsto 1} = 0$$