Elliptic Curves and the Hopf Fibration

Nadir Hajouji[1] and Steve Trettel[2]

[1]Boston, MA, USA; nhajouji@gmail.com
[2]University of San Francisco, CA, USA; strettel@usfca.edu

Abstract

By combining tools from different areas of mathematics, we obtain 3D visualizations of elliptic curves over different fields that faithfully capture the underlying algebra and geometry.

Introduction

This paper is about visualizing elliptic curves. If you've never heard of an elliptic curve, here's all you need to know: 1) They are not ellipses, 2) you might not recognize them as curves, 3) they are *incredibly* interesting, appearing across mathematics, cryptography, and physics and 4) they are *notoriously* hard to explain to non mathematicians. Although they can be defined in simple terms, the modern definition does very little to explain their ubiquity, or exhibit their beauty.

We want to show you what elliptic curves really look like. Using tools from complex analysis, algebra, number theory and topology, we bring these curves into view as 3D renders, and produce a gallery showcasing their diversity. We aim to make elliptic curves accessible to newcomers, and to reveal their aesthetic beauty to a mathematical audience, who met them first through symbols on a page.

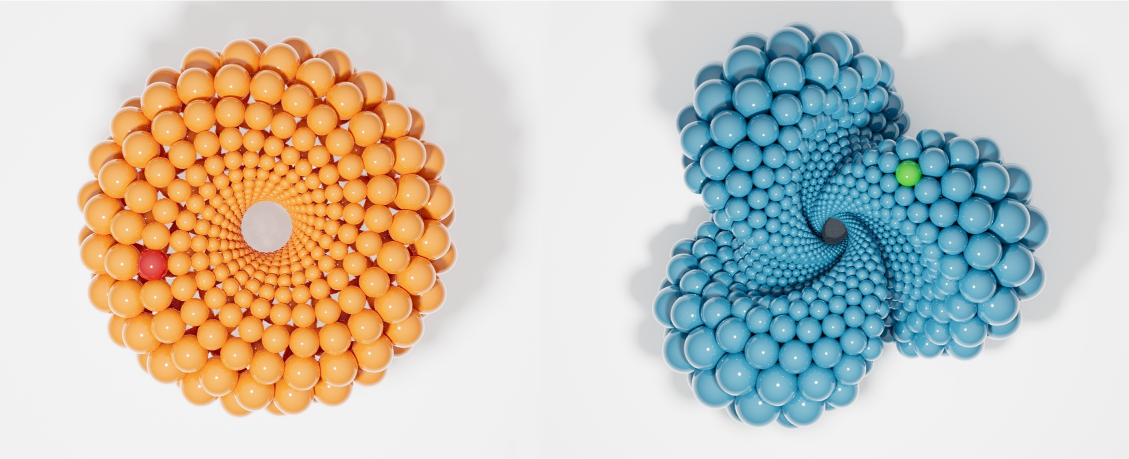

Figure 1: *The elliptic curves $y^2 = x^3 + 3x$ over $\mathbb{F}_{625}$ (orange), and $y^2 = x^3 + 3$ over $\mathbb{F}_{2401}$ (blue).*

What is an Elliptic Curve?

Everyone knows what a curve is, until they have studied enough mathematics to become confused.
— F. Klein[1]

[1] The idea to use quotations to start our sections, as well as the quotes themselves, came from [6].

When a classical geometer says the word “curve,” they mean *something you can draw on a (possibly infinite) piece of paper with a pen*. The unifying concept is “one dimensionality”: each point on the curve has a left and a right, each moment during its drawing a before and an after. In modern mathematics, the word *curve* may refer to any one dimensional object —anything that can described by a single variable. The invention of abstract algebra has allowed us the freedom to consider variables over many wild and wonderful number systems, and opened our eyes to a more varied collection of curves. Real curves look familiar, like segments of the number line, but there are also *complex curves*, which trace out something we might more readily recognize as a surface, and curves defined over *“finite number systems”*, which look like a cloud of isolated points. All of these are equally curves in the eyes of an algebraic geometer: a “single variable object” across different mathematical universes. It is in this modern, tolerant sense that elliptic curves are curves; seeking a unifying perspective for this varied family is one of our mathematical and artistic motivations.

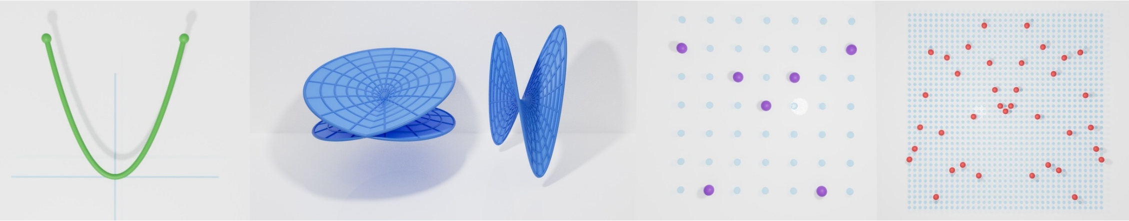

Figure 2: *The curve $y = x^2$ over $\mathbb{R}$ (green), over $\mathbb{C}$ (blue: two views, projecting to three dimensions by deleting the imaginary component of x or y), and over finite fields: $\mathbb{F}_7$ (purple), $\mathbb{F}_{37}$ (red).*

Perspectives on the Circle

Circles are perhaps the most familiar examples of mathematical curves, and we will see that elliptic curves are a natural generalization of circles. To make the similarity between the two more apparent, we start by answering the following question —*how do you describe a circle in algebraic language?* We will give 3 distinct ways of describing the unit circle, and subsequently show that elliptic curves can be defined by tweaking any of those 3 descriptions. The first description, due to Pythagoras and Descartes, is via an equation: the unit circle is the set of solutions $x, y \in \mathbb{R}$ to $x^2 + y^2 = 1$. The second description is via a parametrization: the solutions to this equation coincide with the values of $(\cos\theta, \sin\theta)$ as θ varies across the set of real numbers. Of course, we don’t need to use every real number —replacing θ by $\theta + 2\pi m$, where m is any integer, does not change the point, so we really only need θ between 0 and 2π, or between $-\pi$ and π. This leads to our third description: points θ on the circle are like real numbers, except subject to the condition that they “do not change” if we add integer multiples of 2π. That is, the circle is made out of “ill defined real numbers”: or numbers whose values only makes sense up to this $\pm 2\pi n$ ambiguity. Mathematicians write such numbers as $\mathbb{R}/2\pi\mathbb{Z}$, and more generally G/H (read *G mod H*) for elements of G which are ambiguous up to elements of H.

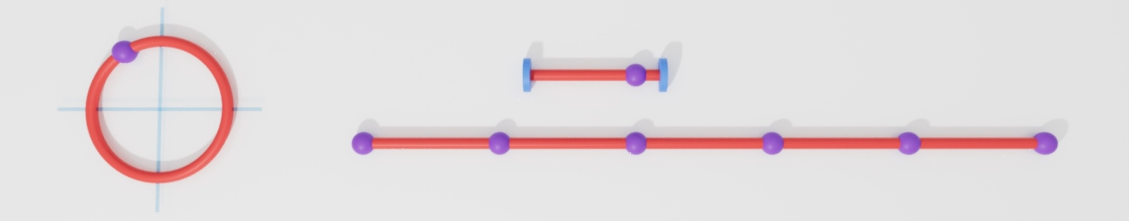

Figure 3: *A circle three ways: (1,2) an implicit / parametric plane curve in $\mathbb{R}^2$ (left); (3) an ill-defined real number in $\mathbb{R}/2\pi\mathbb{Z}$ as a periodic point in $\mathbb{R}$ or element of a fundamental domain (right).*

Elliptic Curves

Elliptic curves are one of the simplest shapes, other than circles, that can be described in each of these three ways. Our starting point will be a generalization of (3): we replace the real numbers by complex numbers, the set of integer multiples of 2π by a lattice $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$, and define an elliptic curve to be the set of ”ill-defined complex numbers” $\mathbb{C}/\Lambda$. Topologically such numbers form a *torus*: a quite natural generalization of the circle indeed! From this starting point, we can build back the other perspectives of our triad. The analog of $\cos\theta, \sin\theta$ for an elliptic curve are the functions $\wp_\Lambda, \wp'_\Lambda$, known as the *Weierstrass $\wp$-function* $\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\lambda-\Lambda-\{0\}} \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}$ and its derivative $\wp'_\Lambda(z) = -2\sum_{\lambda\in\Lambda} \frac{1}{(z-\lambda)^3}$ They satisfy an equation of the form:

$$\left(\frac{\wp'_\Lambda(z)}{2}\right)^2 = \wp_\Lambda(z)^3 + \left(15 \sum_{\lambda\in\Lambda-\{0\}} \frac{1}{\lambda^4}\right)\wp_\Lambda(z) + \left(35 \sum_{\lambda\in\Lambda-\{0\}} \frac{1}{\lambda^6}\right) \tag{1}$$

Calling the infinite sums appearing in this differential equation f_Λ and g_Λ respectively, we see that $(x, y) = (\wp, \frac{1}{2}\wp')$ satisfy the algebraic equation $y^2 = x^3 + f_\Lambda x + g_\Lambda$. This is called the equation of the elliptic curve.

The appearance of these constants f_Λ, g_Λ reveals an important fact: unlike circles, elliptic curves come in *different flavors*. While there is essentially only one circle (any two are equivalent up to scaling), there are many distinct lattices in the complex plane that are not related by scaling or rotation. The corresponding elliptic curves inherit distinct personalities from their lattice progenitors. This additional source of variety is part of what makes elliptic curves such a compelling subject for visual art.

Visualizing Classical Elliptic Curves

We all know that Art is not truth. Art is a lie that makes us realize truth, at least the truth that is given us to understand. The artist must know the manner whereby to convince others of the truthfulness of his lies.
— P. Picasso

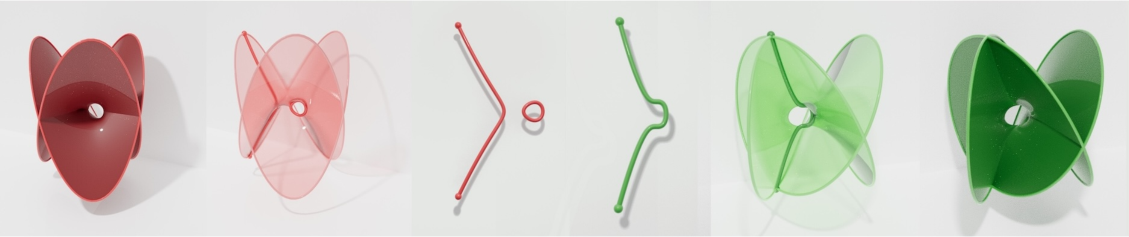

Figure 4: *Equation-based illustrations of elliptic curves, for the curves $y^2 = x^3 - x$ (red) and $y^2 = x^3 + 1$ (green). These illustrations obscure the underlying torus geometry.*

Having the equations defining elliptic curves readily available, it is tempting to try plotting the solutions, much as one does to visualize the circle. There’s just one small problem: x and y are complex, so the points (x, y) live in a *four dimensional space*. For our three dimensional brains, one must then either throw away a dimension (introducing artificial self-intersections), or discard most of the shape, plotting a two dimensional *real slice*. Such images can be seen in Figure 4.

A goal of this paper is to present an alternative approach to visualizing elliptic curves, using their description as quotients $\mathbb{C}/\Lambda$. This is summarized in Figure 5: beginning with an infinitely repeating grid, one may produce a finite visualization by selecting a fundamental domain, although this comes at a cost: the edges of the chosen domain introduce arbitrary discontinuities, sacrificing symmetry and visual elegance. A more compelling alternative to these flattened images would seamlessly “roll up” this repetition onto a smooth toroidal surface, analogous to wrapping a repeating real line around a circle. Constrained by our biology and the local laws of physics, we seek a means of doing this in three dimensions (as opposed to the mathematically natural four-dimensional candidate $(\wp, \wp')$).

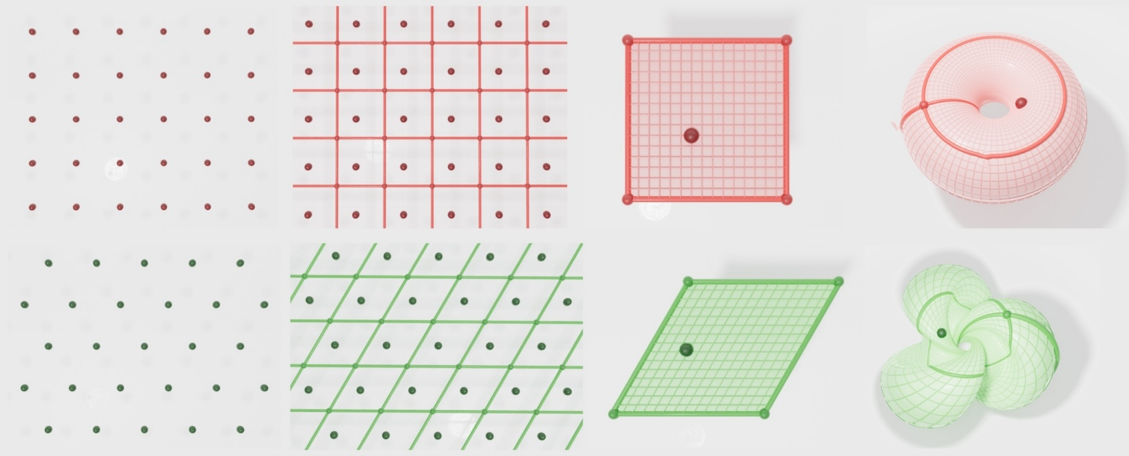

Figure 5: *A point on an elliptic curve: three views (1) as lattice (2) in fundamental domain (3) rolled up. The same elliptic curves as the previous illustration.*

Hopf to the Rescue

While constructing such a ”roll up map” into three dimensions, we must be mindful not to destroy the distinct personalities imbued by their different underlying lattices. Complex geometry tells us any allowable map $\mathbb{C}/\Lambda \to \mathbb{R}^3$ must be angle-preserving (conformal): a strong constraint which means we can't just roll $\mathbb{C}/\Lambda$ up as a torus of revolution, for instance. One natural source of conformal maps is *isometries*, so one might hope to seek an isometric embedding $\mathbb{C}/\Lambda \to \mathbb{R}^3$. Unfortunately a classic argument in differential geometry says we cannot do this: there are no flat tori in $\mathbb{R}^3$ and thus no isometries from $\mathbb{C}/\Lambda$ into $\mathbb{R}^3$. However one can save the idea with a small tweak: since stereographic projection is conformal, it would be enough to find flat tori into the 3-sphere, and then map them into $\mathbb{R}^3$ by a composition of conformal maps!

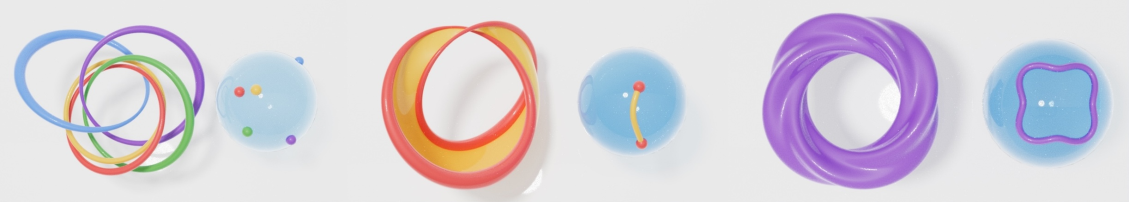

Figure 6: *Point preimages under the Hopf fibration are circles, so the preimages of curves are annuli or tori.*

Amazingly, such flat tori exist and were were described by Ulrich Pinkall in [4]. The key tool is the Hopf fibration, a topologically nontrivial map $\eta\colon \mathbb{S}^3 \to \mathbb{S}^2$ defined by $\eta(z, w) = z/w$ for unit vectors $(z, w) \in \mathbb{C}^2$, with z/w interpreted as a point on the Riemann sphere $\mathbb{C} \cup \infty$. This simple formula conceals beautiful geometric structure: each point's preimage is a circle, so an arc lifts to an annulus, and a closed curve to a torus. A straightforward calculation shows that these tori are flat, setting up a correspondence between tori $\mathbb{C}/\Lambda$, and closed curves on the 2 sphere. Pinkall makes this explicit, showing the preimage $\eta^{-1}(C)$ of a simple closed curve C on $\mathbb{S}^2$ of length L enclosing area $A < 2\pi$ is isometric to $\mathbb{C}/\Lambda$, for $\Lambda = 2\pi\mathbb{Z} \oplus (\frac{A}{2} + i\frac{L}{2})\mathbb{Z}$. Thus, to realize an elliptic curve $\mathbb{C}/\Lambda$, we need only find a loop on the sphere with the appropriate A and L.

Fixing area and length still leaves a generically infinite dimensional space of possible curves, which provide substantial artistic freedom in constructing embeddings. After choosing an appropriate curve C, the real computation begins: we need the isometry $\mathbb{C}/\Lambda \to \eta^{-1}(C)$. We sketch this below, slightly

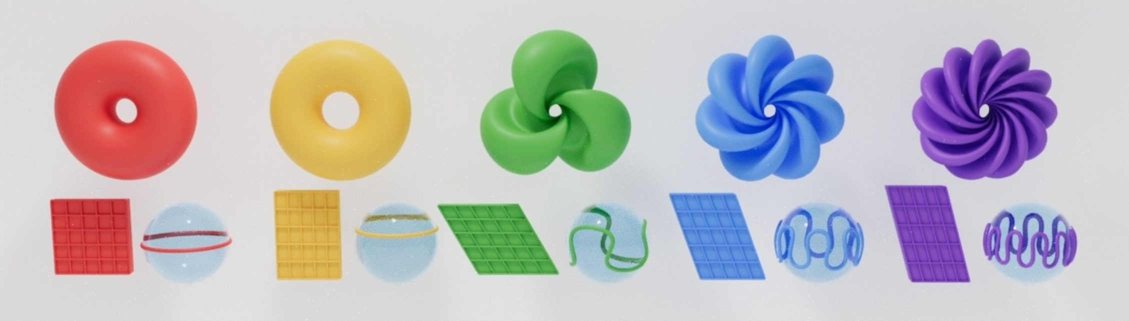

Figure 7: *Lattices generated by* 1 *and* $\tau \in \{i, i\sqrt{2}, \frac{1+i\sqrt{3}}{2}, \frac{1+i\sqrt{7}}{2}, \frac{1+i\sqrt{11}}{2}\}$*, curves on the sphere with the corresponding lengths and areas, and the resulting embedded elliptic curves in* $\mathbb{R}^3$.

generalizing the techniques of [1]. Parameterizing C by $(\theta(t), \phi(t))$ and the Hopf fiber above $(\theta, \phi) \in \mathbb{S}^2$ as $H_{(\theta,\phi)}(s) = (e^{i(\theta+s)} \sin \frac{\phi}{2}, e^{is} \cos \frac{\phi}{2})$ we can parameterize the torus $\eta^{-1}(C)$ by $s + it \mapsto H_{c(t)}(s)$ in $\mathbb{S}^3$. While this initial parameterization is not an isometry, we modify it into one by accounting the curvature of the Hopf fibration (as a circle bundle over $\mathbb{S}^2$), and then compose with stereographic projection into $\mathbb{R}^3$. To save others the trouble of computing this, we give the resulting map $\mathbb{C}/\Lambda \to \mathbb{R}^3$ below:

```
Given $s + it \in \mathbb{C}$ with $t < L/2$ and a curve $(\theta(x), \phi(x))$ on $\mathbb{S}^2$:
Numerically find $v$ such that $L(v) = \int_0^v (\theta'(x)^2 \sin^2 \phi(x) + \phi'(x)^2)^{1/2}\, dx = 2t$
Compute $\theta = \theta(v)$, $\phi = \phi(v)$ and $f = \int_0^v \sin(\phi(x)/2)\, \theta'(x)\, dx$
Compute $h = H_{(\theta,\phi)}(s - f) = (e^{i(\theta+s-f)} \sin \frac{\phi}{2}, e^{i(s-f)} \cos \frac{\phi}{2})$
Return stereographic projection $\sigma(h)$ for $\sigma\colon (x, y, z, w) \mapsto (x, y, z)/(1 - w)$
```

Elliptic Curves over Other Number Systems

Algebra is the offer made by the devil to the mathematician. The devil says: I will give you this powerful machine, it will answer any question you like. All you need to do is give me your soul: give up geometry and you will have this marvelous machine. — M. Atiyah

Taking the modern mathematician's notion of curve seriously, we have become well acquainted with many donut-shaped elliptic curves. But these are just one lineage in the vast elliptic curve family: to meet others, we must learn how to swap $\mathbb{C}$ for other number systems. This requires using a different part of our triad: we will need the equation of the elliptic curve. Given a number system k, an *elliptic curve over* k is the solutions $x, y \in k$ to an equation of the form $y^2 = x^3 + fx + g$. We might then hope to visualize these new curves by plotting their solutions in $(x, y) \in k^2$ (at least when we can reasonably visualize k). We've actually already seen such plots for $\mathbb{R}$ in Figure 4, and plots over finite number systems look like scatterings of dots akin to Figure 2. This may give the impression that the family resemblance between the various lineages of elliptic curves ends with their equation. But that is not the case: despite vast algebraic differences, a deep geometric unity lurks beneath the surface. Looking over many fields, we'll find that classical elliptic curves survive in the background like ghosts, subtly influencing their structure.

Our goal in this section is to realize this unified view, and render images across the elliptic curve family that highlight familiar toroidal shapes and lattice-like symmetries. To do so we employ Galois theory —an advanced toolkit from algebra that was developed by one of the romantic heroes of mathematics.[2] Galois teaches us: *the key to understanding algebra over small number systems lies in understanding symmetries of*

[2] Indeed, Galois came up with the tools we need when he was a mere 16 yeas old. His genius was lost to the world after his untimely death in a duel at the tender age of 20.

larger number systems, like the complex numbers.

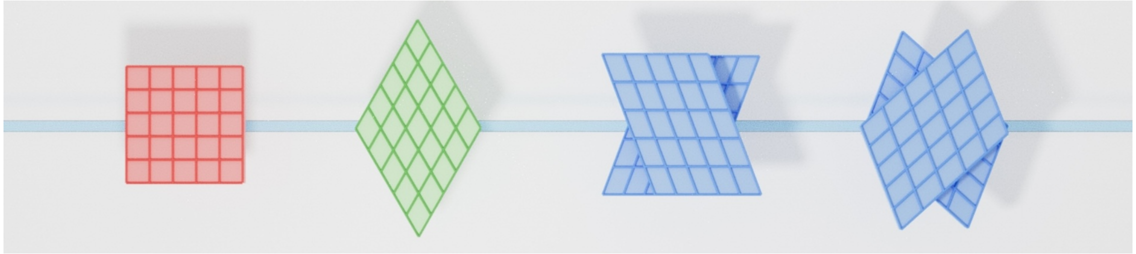

Figure 8: *A pair of "real" lattices (red, green). "Non-real" (i.e. complex) lattices (blue) have no reflection symmetry, in any orientation.*

We explain this cryptic decree via example, using Galois' insight to find real elliptic curves among the complex tori we already understand. Our first step is to realize one can talk about $\mathbb{R}$ inside of $\mathbb{C}$ using the language of symmetry: real numbers are precisely those that are *unchanged* by complex conjugation. With some work [3][5], we can show that this gives a way to discover which complex curves have a real elliptic curve hiding inside them —the ones whose lattices are unchanged by reflection in the x-axis (the geometric realization of this complex conjugation symmetry), see Figure 8. And once we've sorted these out, we can further uncover the *points* of the hidden real curve itself by seeing what is fixed by complex conjugation in $\mathbb{C}/\Lambda$. These include the x axis, as well as points z related to $\bar{z}$ by a lattice element. With the points in hand, we can depict the real curve inside its complex counterpart using the *roll-up* map derived from the Hopf fibration, or recover the standard illustration in $\mathbb{R}^2$ via the parameterization $(\wp_\Lambda, \wp'_\Lambda)$, see Figure 9.

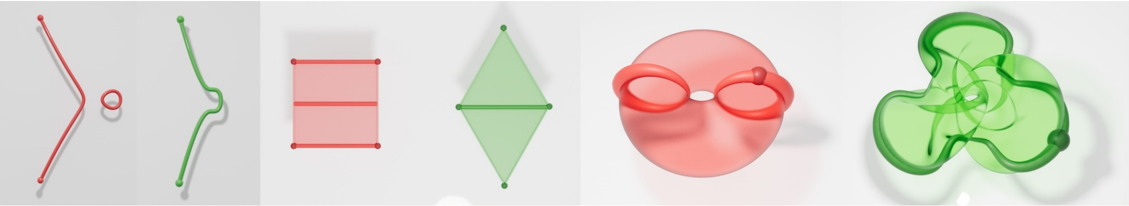

Figure 9: *The real elliptic curves $y^2 = x^3 + 3x$ (red) and $y^2 = x^3 + 1$ (green), as standardly depicted as solutions in $\mathbb{R}^2$ (left), and as subsets of a classical elliptic curve $\mathbb{C}/\Lambda$ (center, right). The standard illustrations close up via a point at infinity, highlighted as a finite point when embedded in $\mathbb{C}/\Lambda$.*

Galois' philosophy can also be used to visualize elliptic curves over much smaller number systems called *finite fields*. If these are new, don't worry about the details —all you need to know is that the symbol $\mathbb{F}_q$ denotes a "number system" that contains precisely q numbers, including some familiar ones like $0, 1, 2...$ To seek out the $\mathbb{F}_q$ elliptic curves hiding among the complex ones, we will again look for those with a special symmetry: the analog of complex conjugation for $\mathbb{F}_q$, known as *the Frobenius*. As a result of some beautiful mathematics [2][3][5], we can show that this map is simple to compute when we represent our curves as $\mathbb{C}/\Lambda$, acting as "multiplication by a complex number". Upon finding a complex curve with this symmetry, we uncover the hidden $\mathbb{F}_q$ points by seeing what the Frobenius fixes, as in Figure 10. This allows us to draw pictures of the $\mathbb{F}_q$ curve on our familiar complex tori —even though $\mathbb{F}_q$ is not a subset of $\mathbb{C}$! Furthermore, each lattice-complex number pairing is unique to the elliptic curve, so we obtain a unique picture for each curve.

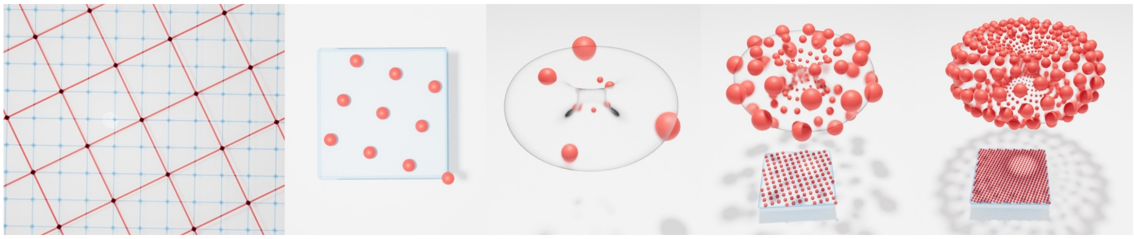

Figure 10: *For the elliptic curve* $y^2 = x^3 + 3x \pmod 5$*, the Frobenius looks like "multiplication-by-*$(-2+i)$*" on the square lattice (far left). We find the* $\mathbb{F}_5$ *points by identifying the fixed points of Frobenius (center, on fundamental domain and rolled up), and we similarly we obtain the* $\mathbb{F}_{125}$*,* $\mathbb{F}_{625}$ *points by identifying fixed points of suitable powers of Frobenius (right).*

A Gallery of Elliptic Curves over Finite Fields

"Should you just be an algebraist or a geometer?" is like saying "Would you rather be deaf or blind?"
— M. Atiyah.

At this point in the story, our training as mathematicians compels us to explain precisely how we're using Galois theory to make our pictures, and how we know our method always works. We will answer these questions in a later work, and for now, content ourselves with sharing the end result of our labor: new illustrations of elliptic curves over finite fields, living inside the ghost of the complex elliptic curve that once gave birth to it.

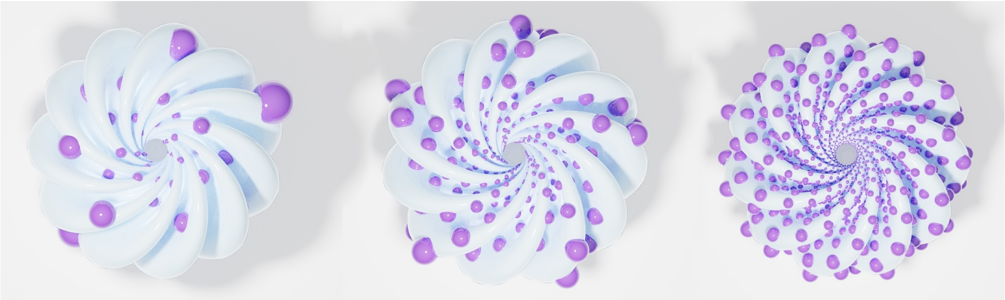

Figure 11: *The elliptic curve* $y^2 = x^3 + x + 1 \pmod 5$ *over* $\mathbb{F}_{125}$ *(left),* $\mathbb{F}_{625}$ *(middle) and* $\mathbb{F}_{3125}$ *(right).*

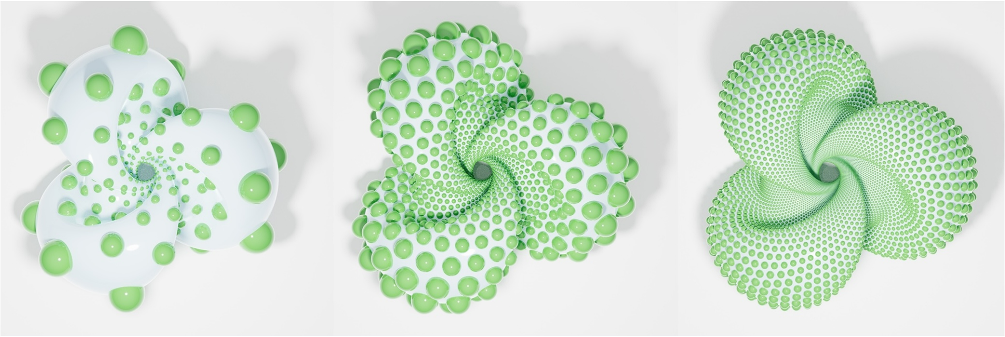

Figure 12: *Points of* E: $y^2 = x^3 + 3 \pmod 7$ *over the fields* $\mathbb{F}_{343}$ *(left),* $\mathbb{F}_{2401}$ *(center) and* $\mathbb{F}_{16,807}$ *(right).*

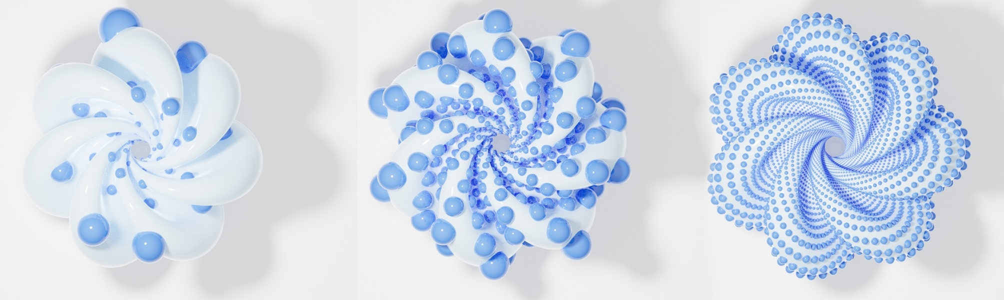

Figure 13: *The elliptic curve* $y^2 = x^3 + 5x + 7 \pmod{11}$ *over* $\mathbb{F}_{121}$ *(left),* $\mathbb{F}_{1331}$ *(middle) and* $\mathbb{F}_{14,641}$ *(right).*

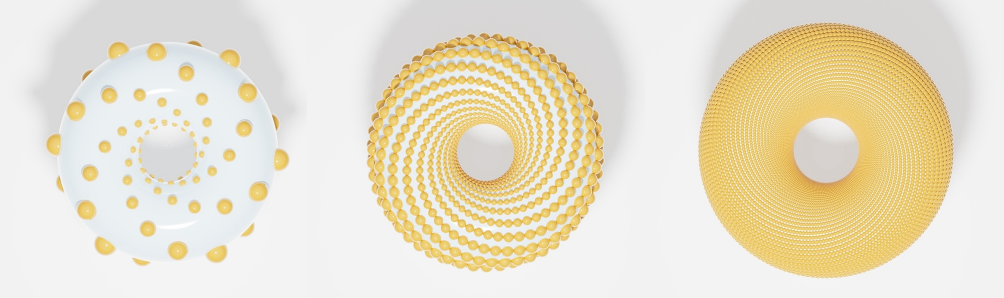

Figure 14: *The elliptic curve* $y^2 = x^3 + x + 3 \pmod{11}$ *over* $\mathbb{F}_{121}$ *(left),* $\mathbb{F}_{1331}$ *(middle) and* $\mathbb{F}_{14,641}$ *(right).*

Conclusion

In the course of writing this paper, we realized that we would have to answer the following question —*How do we choose the elliptic curves to include in the paper?* There are infinitely many to choose from, each with its own unique personality, more than we can ever hope to see in our finite lifetimes, and we have only 8 pages. We shared some of our favorites —but we have a lot more to show!

The true beauty that enthralls mathematicians lies in the patterns that emerge when one looks at *lots* of elliptic curves. You can think of elliptic curves as musical notes—we've hopefully convinced you that they "sound different" from each other, but just like musical notes, they can only do so much when played in isolation. We invite you to visit our website [3], where you can see a larger (though always incomplete) gallery and learn about the beautiful mathematics behind our pictures.

References

[1] T. Banchoff. "Geometry of Hopf Mapping and Pinkall's Tori of Given Conformal Type." *Computers in Algebra*. New York, 1990. pp. 57–62.

[2] D. A. Cox. *Primes of the form* $x^2 + ny^2$. ser. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989. Fermat, class field theory and complex multiplication.

[3] N. Hajouji and S. Trettel. "Visualizing Elliptic Curves: Extended Gallery and Companion Papers." https://www.elliptic-curves.art/.

[4] U. Pinkall. "Hopf tori in S3." *Inventiones Mathematicae*, vol. 81, 09 1985, p. 379.

[5] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Springer, 1994. vol. 151.

[6] R. Vakil. "The Rising Sea: Foundations Of Algebraic Geometry Notes." https://math.stanford.edu/~vakil/216blog/.