# *Hyperelliptic Threshold Noise*
# A Mathematician's Perspective

Jennifer Johnson-Leung

## 1 Overview

The prints in this exhibition were created from plots of the points on a single hyperelliptic curve over different finite fields of prime order. The purpose of this essay is to explain what hyperelliptic curves and finite fields are and to say a bit about how they relate to my research. I will also consider the art of printmaking through a mathematical lens.

## 2 Some Background

The mathematics that I study is an area broadly known as number theory. My research sits at the intersection of arithmetic geometry and automorphic representation theory. I want to begin with a very old question: "When does a polynomial equation have integer (or whole number) solutions?" This may already sound esoteric, but the Babylonians cared about this question for engineering purposes long before Diophantus of Alexandria brought a mathematical treatment to the problem.

Babylonian tablets enumerated integral solutions to the equation $x^2 + y^2 = z^2$, because that is the relationship between the lengths of the sides of a right triangle. A nearly 4,000 year-old tablet listing these solutions (sometimes called Pythagorean triples) was donated to Columbia University by the archaeologist George Plimpton in the 1920's.

A student in an Algebra 2 class could prove that there are infinitely many Pythagorean triples, given the appropriate hints. In fact, you probably know some of the triples like $(3, 4, 5)$ or $(5, 12, 13)$. But many non-mathematicians are surprised to learn that polynomial equations often have very few or even no solutions in the integers. For example, if $n \geq 3$, the equation $x^n + y^n = z^n$ has no integer solutions unless you set one of the three variables to zero. For over 300 years, mathematicians believed this fact known as Fermat's Last Theorem, but despite many attempts, noone was able to prove it. The errors in their thinking led to the development of modern algebraic number theory during the eighteenth and nineteenth centuries.

The proof that was completed by Andrew Wiles in 1995 used a very indirect line argument by proving a statement called the *modularity theorem*. The modularity theorem states that given an elliptic curve (a curve given by an equation of the form $E : y^2 = x^3 + ax + b$ with $a$ and $b$ rational numbers) there is a special function called a modular form which encodes the number of solutions to $E$ over finite fields. How the modularity theorem proves Fermat's last theorem is a story for another time, and there have been many books written on this subject.

The part of my research that germinated the striking prints in the exhibition is concerned with a generalization of the modularity theorem called the *paramodular conjecture*. This conjecture generalizes the modularity theorem and predicts a similar relationship between genus 2 hyperelliptic curves and special functions called Siegel paramodular forms. In the paragraphs that follow, I will explain some of the mathematical objects that we have used in this work and their connections to my research. All of the mathematical terms have very precise definitions and fascinating interconnections, but our focus in this essay is on intuition and on appreciation of the beauty of number theory.

# 3 Finite Fields

Finite fields occur in the world around us with surprising frequency. They are a basic building block of our modern computer security system, underlying key exchange protocols, for example. In mathematics, a field is a set that is closed under addition, subtraction, multiplication, and division, so that if I perform those operations on two numbers in the set, the result is also in the set (except for dividing by zero, which is never allowed). For example, the rational numbers (fractions) form a field as does the set of all real numbers (the number line). An important non-example is the set of integers. The integers do not form a field because if you divide 3 by 4, for example, the result is not an integer. There are many more examples of fields in mathematics, and most of them (as with our examples above) have infinitely many elements. There are also fields with a finite number of elements. In fact, we have the following theorem.

**Theorem 3.1.** *Let $F$ be a finite field. Then there is a prime number $p$ and a positive integer $n$ so that the number of elements in $F$ is $p^n$. Conversely, if $p$ is a prime number and $n$ is a positive integer then there is a field $F$ with $p^n$ elements which is unique (up to isomorphism).*

This theorem says that there is exactly one finite field for every prime power. For our prints, we focused on fields that have a prime number of elements (so $n = 1$). For these fields, the rules for addition and multiplication can be explained in terms of modular arithmetic. Consider the prime number 7. We can calculate 6+5 modulo 7 by calculating the remainder when dividing $(6 + 5)$ by 7. So,

$$6 + 5 = 11 = 4 \bmod 7 \qquad \text{and} \qquad 6 * 5 = 30 = 2 \bmod 7$$

. Notice that $6 = -1 \bmod 7$ and $5 = -2 \bmod 7$, so you can also look at this as saying that

$$(-2) + (-1) = -3 = 4 \bmod \qquad \text{and} \qquad (-1) * (-2) = 2 \bmod 7$$

. A basic result that makes these calculations possible is that the answer does not depend on *when* you reduce modulo 7. Below are the multiplication and addition tables modulo 7. You can see that every number has both an additive and a multiplicative inverse and that 6 really does behave as $-1$.

| + | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 0 |
| 2 | 2 | 3 | 4 | 5 | 6 | 0 | 1 |
| 3 | 3 | 4 | 5 | 6 | 0 | 1 | 2 |
| 4 | 4 | 5 | 6 | 0 | 1 | 2 | 3 |
| 5 | 5 | 6 | 0 | 1 | 2 | 3 | 4 |
| 6 | 6 | 0 | 1 | 2 | 3 | 4 | 5 |

| × | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 0 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 0 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 0 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 0 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 0 | 6 | 5 | 4 | 3 | 2 | 1 |

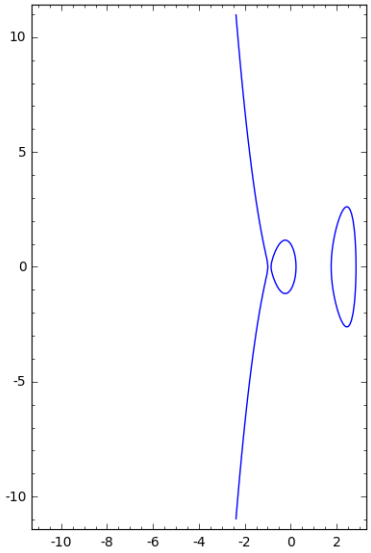
# 4 A Hyperelliptic Curve

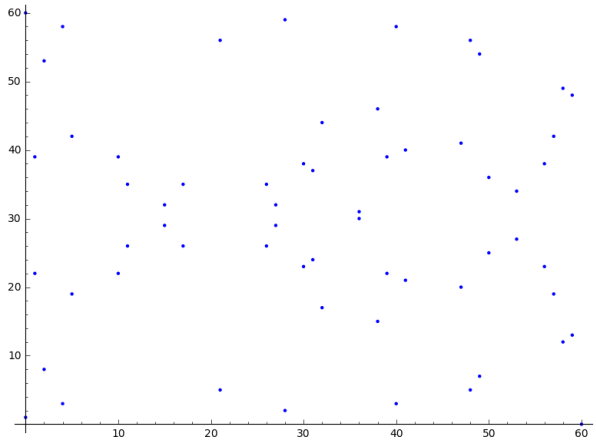
The second object that we want to consider is called a *hyperelliptic curve*. These curves are given by equations of the form $y^2 = f(x)$, where $f$ is a polynomial of degree at least 3. These curves can also be used to create cryptosystems, and you have probably used many of them when shopping online or logging in to a secure site. Hyperelliptic curves have an invariant attached to them called the *genus* of the curve. The elliptic curves studied by Wiles in his proof of the modularity theorem are hyperelliptic curves of genus 1. The curves that appear in my research are mostly of genus 2. This means that if I plot the curve over the complex numbers, it will look like a doughnut with two holes in it.

The equation for the curve that germinated the prints in the *Visualizing Science* exhibition is relatively simple:

$$y^2 = -x^5 + 3x^4 + 2x^3 - 6x^2 - 3x + 1.$$

Consider the plots of the curve below




The plot on the left is the solution set to this equation over the real numbers. The plot on the right is over the finite field with 61 elements. The stencils for the prints derived from the plots of the curve over fields of order 47, 61, 211, 223, 541, 1013, and 1571. It is easy to see that both of these plots have a horizontal line of reflection which comes from the $y^2$ term of the equation. This symmetry occurs because for every solution $(x_0, y_0)$ to the equation, $(x_0, -y_0)$ is also a solution since $y^2 = (-y)^2$. This curve also has extra symmetries which we call complex multiplication. It is of interest to my work as one of only a handful genus 2 curves with rational coefficients that have this property of complex multiplication, which also guarantees that the curve is paramodular.

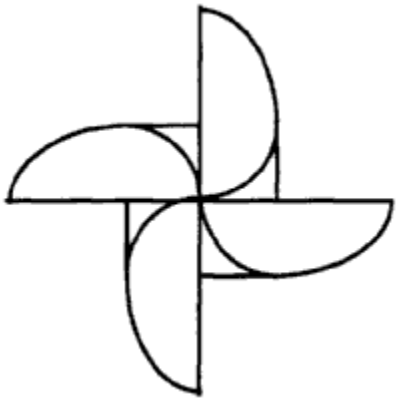
# 5 A Mathematical View of Printmaking

As part of this project, I had the privilege of watching Mike Sonnichsen create prints. Printmaking is a multistep process in which the products of one step are the tools for creating the next. Using the plots discussed in the previous section, Mike modified the points to be of printing scale and created 8 stencils. (The astute reader might be frowning at this point as I only listed 7 prime numbers in the overview, but this is not a mistake. Two distinct stencils were created from the plot over the finite field with 1571 elements.)

Watching Mike use these stencils to print, brought to mind the mathematical idea of a function. Children begin to learn about functions in school at a fairly early age, and you

may remember some from your own school years such as the sine function or the exponential function. But the idea of a function in mathematics is much more general. Given any two collections of objects (called sets) a *function* is a mapping from one of the sets to the other so that for any given input there is an output, and if I put that input in again, I would get the same output again. In this way, each stencil might be thought of as a function from the set of inks to the set of images. It is interesting to me that if I wanted to be very rigorous, then the stencil would fail to satisfy the definition of function because each print is distinct from the others even when using the same color and the same stencil. The real world is too messy to satisfy strict mathematical definitions.

Printmakers also establish protocols for their work. For this project, Mike decided that each choice of color and stencil would be printed four times on the paper in a rotational pattern. This has the effect of overlaying each plot on itself, breaking the reflectional symmetry present in the original plots, and replacing it with a rotational symmetry. The image below gives an example of rotational symmetry. These protocols remind me of the axioms that govern mathematical inquiry. Axioms are assumed truths, and like a print-maker's protocols they provide structure to mathematical inquiry. Even with these protocols, the number of possible prints from the stencils and the inks is enormous. Let's calculate the size of the sample space. We have 8 stencils, 10 inks, and 10 printing rounds. For each printing round, we have $10 \times 8 = 80$ possible choices for the image since we might choose to repeat a stencil or a color. As we are printing 10 times, the total number of possible final images is $80^{10} = 10737418240000000000$. To understand how big this number is, consider that if we laid out all of these prints side by side, we could over the surface of the earth about eight thousand times! In this way, I see our printmaker as an explorer, winding his way through the vast sample space seeking out images that surprise, engage, or perhaps even move the viewer.



If you would like to know more about the math discussed here, please contact me at `jenfns@uidaho.edu`. You can also hear more at the Renfrew Interdisciplinary Colloquium on March 28 at the University of Idaho.