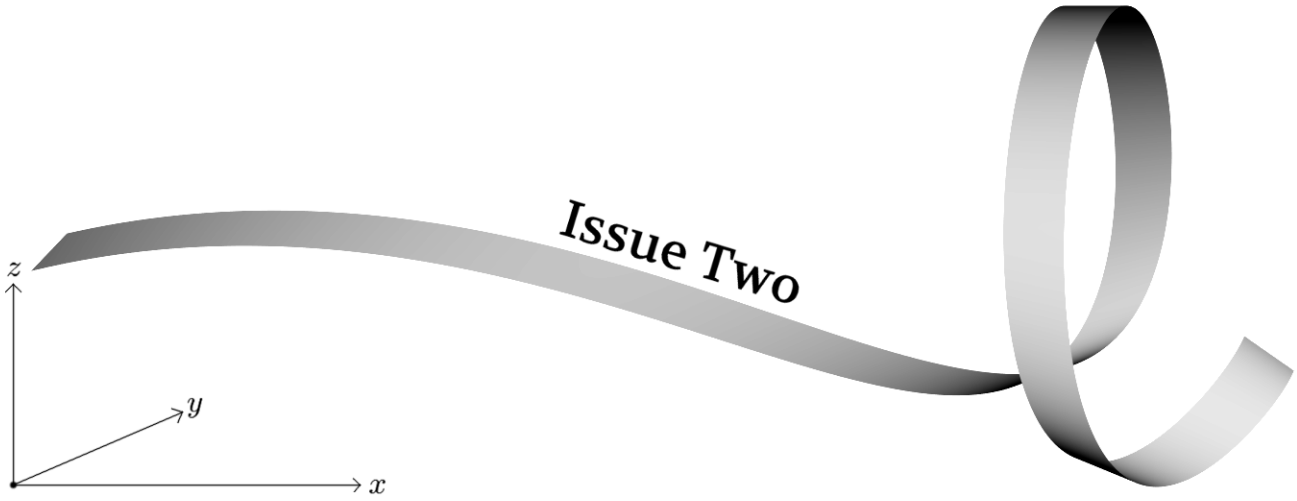
The MathILy Record of Mathematics



$$x = \tfrac{1}{4}u^5 - \tfrac{3}{10}u^4 - \tfrac{17}{10}u^3 + \tfrac{1}{5}u^2 + u + v\cos\left(\tfrac{2}{5}u\right) + 7$$

$$y = \sin(3u) + u + 2$$

$$z = \cos\left(\tfrac{3}{2}u\right) + \cos\left(\tfrac{7}{2}u\right) + v\sin\left(\tfrac{2}{5}u\right) + \tfrac{1}{2}$$

$$-\tfrac{3}{2} \leq u \leq 2$$

$$0 \leq v \leq \tfrac{2}{5}$$

cover design by Sean Harrigan

Monday's Daily Gather - Brian
Fibonacci Numbers. Period.

by Nick

Brian began the talk by asking us if, given $n \in \mathbb{N}$, there is a Fibonacci number divisible by n. We decided to consider Fibonacci numbers mod n, since then a value of zero in mod n would indicate that the number is divisible by n. Next, We looked at patterns in the values of each Fibonacci number in mod n. For example, Fibonacci numbers in mod 2 are $0, 1, 1, 0, 1, 1, \ldots$ In mod 3: $0, 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, 0, 2, 2, 1, \ldots$..Then we counted how many numbers were in each sequence before it repeated and built a table:

n	Period
1	1
2	3
3	8
4	6
5	20

To denote the first number in the Fibonacci sequence we used $F_0 = 0$, $F_1 = 1$, $F_2 = 1$, $F_3 = 2$, $F_4 = 3$, and so on. We realized that by using how many numbers were in the Fibonacci sequence mod n, denoted by k where $k \in \mathbb{N}$, they could figure out what Fibonacci numbers were divisible by n. We found the kth Fibonacci number, or F_k, is divisible by n and extended this conjecture to F_{kx} for $x \in \mathbb{N}$. For example, in mod 3 there are two 0s in the sequence before it repeats. So, by the first conjecture, F_{8x} is divisible by 3, and because of the second zero in the sequence $F_{8x} + 4$ is divisible by 3 as well, which when combined gives us that F_{4x} is divisible by 3.

Next we looked at finding a pattern within the numbers of repeating cycles. A few claims were made about this. For example, Hussain claimed that if the period of some power of prime n is k, then the period of na is $n^{a-1}k$. For example, suppose $n = 2$, we find $k = 3$, if we are looking to find the period when $n =$ m4, we see that $4 = 2a$ when $a = 2$. Now applying this claim, we see that $n^{a-1}k$ holds true, because 22-1(3)=6 which is the period of 4. Although we did not prove this in class, this remains an open conjecture, though partial results are known.

Another conjecture that we made was that if $\gcd(a, b) = 1$, the period mod ab is the period mod a times the period mod b. We finished the daily gather by proving this statement.

Tuesday's Daily Gather - Emil

Let's Talk Crypto, yo!

by Richard Z.

After giving in-depth commentary on the generic clip art that made up his title slide, Emil began his talk with an analysis on the vulnerability of a physical pin tumbler lock, and explained how lockpicks could be used to crack it. Then, we considered ciphers, or ways of writing plain text into coded ciphertext. The Caesar cipher, the simplest cipher, assigns each letter to its respective number in $\mathbb{Z}_{26}$ (A=1, B=2, and so on) and shifts the entire message by one. Caesar ciphers are not very secure because one can easily decrypt the encrypted messages by looking at the frequencies of each letter within the message. Certain letters within the English language, for example, 'e', are glaringly more frequent.

We improved this method by adding the message's corresponding numbers in $\mathbb{Z}_{26}$ to another message's pre-shift corresponding numbers in $\mathbb{Z}_{26}$. This way, only the recipient, who knows the second message, can decrypt it. This way of encryption is called the one-time pad, and is the most secure. Unless one knows the shared secondary message or has an easy way to obtain it, there are an innumerable amount of unique strings that need to be checked when one is trying to brute force a decryption. However, because this method requires a shared secret message beforehand and the said message needs to be of great length if any meaningful messages want to be encrypted, it is not practical for standard use.

Emil then discussed types of block ciphers, ciphers that take a message and break it up into blocks before encoding them. We learned that if each block of plaintext had the same output, then a pattern would still be distinguishable in the ciphertext. Using this information, we improved the algorithm by combining plaintext and the last block's ciphertext to create the new ciphertext. This way, no distinguishable pattern exists in the final ciphertext message.

We then considered how to create a shared secret between Emil and Tom if they had not communicated beforehand, and were forced to voice their communications to everyone within the room as well. We discussed the Diffie-Hellman (D-H) protocol, which involves picking a very large prime p and an integer g such that g is a primitive root modulo p. Both p and g are publically known. Emil and Tom both choose secret exponents a and b. Emil makes publicly known the number $g^a \pmod p$, and Tom shares the number $g^b \pmod p$. By taking each other's numbers to their own secret exponents, they both arrive at a shared secret number $g^{ab} \pmod p$. Using temporary keys made by this method, one can ensure perfect forward secrecy, where even if the private key is compromised, all past communications remain secret.

In addition, we touched upon public key encryption. In public key encryption, each user has two complementary keys, a public key and a private key. The public key is used by the sender to encrypt the message, and the private key is used by the recipient to decrypt it. However, both public key encryption and the D-H protocol suffer from a problem: while the message is secure, it cannot be verified that the sender is truly who they claim they are. To solve this problem, a trusted third-party, like Verisign, issues signed certificates of authenticity. In order to create these certificates, a user usually needs to physically meet with the third-party.

Wednesday's Daily Gather

Math Movies

by Adam

On Wednesday, as usual, we saw several math movies. There is no doubt that the most interesting one was about the Hilbert Curve — a continuous fractal space-filling curve first described by the German mathematician David Hilbert in 1891. The Hilbert Curve is a slightly simpler version of the Peano Curve, the first example of a space-filling curve discovered in 1890 by Italian mathematician Giuseppe Peano.

One of the possible applications of a Hilbert Curve presented in the movie was translating images to sound which, in fact, is a translation of data that is fundamentally two-dimensional (pixels) to data which is one-dimensional (a collection of frequencies all played at once).

In order to understand how Hilbert Curves work, you need to imagine an arbitrary image. In the movie it was a picture of a lion with 256x256 pixels. Now, each of the pixels needs to be associated with a unique frequency so that the brighter the pixel, the higher the corresponding frequency. Moreover it is important that frequencies which are close together should stay close to each other in the pixel space. This way, even if it was difficult to distinguish between two frequencies, they will each refer to almost the same point in the pixel space. In order to map a 256x256 pixel image, you would have to use a Pseudo Hilbert Curve of order 8.

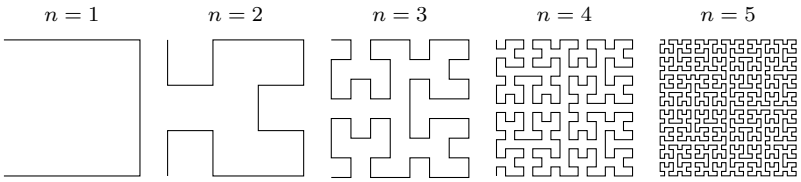


Figure 1: Pseudo Hilbert Curves of order n

Why is the Hilbert Curve better than the "snake curve"?

If you decided to increase the resolution of an image from 256x256 pixels to 512x512 pixels using the "snake curve", many points on the frequency line would go to completely different parts of the pixel space. Consequently, everyone who has already learned how to interpret frequencies would have to relearn how to see with their ears as the frequencies would be now associated with different pixels. By using a Hilbert Curve filling technique, however, each time you increase the order of the Pseudo Hilbert Curve, a given point on the line moves very little and approaches a specific point in the plane.

Why is the Hilbert Curve a space filling function?

1. It is well-defined — points on Pseudo-Hilbert-curves converge
2. It gives a curve — meaning that it is continuous
3. It fills all of space — each point in the unit square is an output of the Hilbert Curve

Other applications of the Hilbert Curve:

The Hilbert Curve is primarily used in computer science. For instance, the range of IP addresses may be mapped into particular image. What is more, the curve helps to compress data warehouses.

Thursday's Daily Gather - Ron Taylor, Berry College
Color Addition Across the Spectrum of Mathematics

by Victor

Moving into the lecture hall in Park 243, MathILy welcomed Professor Ron Taylor from Berry College. Dr. Taylor introduced us to the game *Al-Jabar*, a color-mixing game played with colored stones. The point of the game is to exchange the colors in your hand with equivalent colors from the shared pile to reduce the number of stones in your possession. Color equivalency is determined through an interesting selection of additive and subtractive color-mixing rules.

By our rules, both additive and subtractive mixing use red, yellow, and blue as primary colors, and mixing all three primary colors results in white. Furthermore, we defined a binary structure similar to a light switch such that adding two of the same color resulted in darkness, or black. There are 8 colors in total, red, yellow, blue, orange, green, purple, white, and black.

Dr. Taylor then showed that we could interpret this game mathematically four ways:

1. Algebraically, as a lasket
2. Geometrically, using finite geometry
3. With Vandermonde theory, using stanver coloring
4. Using Set Theory, as a vehicle for the symmetric difference operation, $\triangle$

We were introduced to the lasket, a familiar structure also known as the *woozle*, the *finiruf*, or the *prugo*. We showed that color-mixing in *Al-Jabar* has the properties of closure, associativity, identity, and invertibility, the axioms of a lasket. By representing all 8 colors as a ordered pair of 3 elements from $\mathbb{Z}_2$, and adding them component-wise modulo 2, $\mathbb{Z}_2 \bowtie \mathbb{Z}_2 \bowtie \mathbb{Z}_2$, we in fact obtain the correct color as dictated by our mixing rules.

We then looked at the Fano Plane, a geometry with only 7 points and 7 lines. Each line passes through 3 distinct points, and any pair of lines intersects in exactly 1 point. Represented geometrically, it resembles a triangle with a circle inscribed inside. By coloring the points with the different colors, excluding black, we found that the the sum of any 2 colors on a line was the color of the remaining point. In fact, the sum of all three colors on a line was black, meaning we covered all 8 colors!

In Vandermonde theory, we deal with stanvers, ordered pairs of the set of dowers and the set of brackets, 2-element subsets of dowers. Our readers may also recognize them as *meadow maps* or *spaghetti monsters*. We showed that by representing the Fano Plane as a stanver and performing a total coloring, where no two brackets sharing a dower, or two dowers connected by a bracket could be the same color, the color of an individual bracket or dower was equal to the sum of all incident dowers or brackets, respectively.

Finally, we looked at *Al-Jabar* using set theory. We looked at the symmetric difference operation, $\triangle$, defined as follows: $A \triangle B = (A \cup B) \setminus (A \cap B)$. We can interpret the rules as defining equivalence classes on a power set of all the colors, $\{red, yellow, blue, orange, green, purple, white, black\}$. We can take any equivalent representative of 2 colors, denoted by the sets C_1 and C_2, and perform the symmetric difference operation, $C_1 \triangle C_2 = C_3$ to obtain the result of the mixing of the 2 colors, denoted here by set C_3.

To close off the lecture, Dr. Taylor and Rob played a friendly game of *Al-Jabar*, which ended in a close draw.

Friday's Daily Gather - Dylan Shepardson, Mount Holyoke College
Linear Programming

by Jordan

Dylan posed an optimization problem to us that goes as follows:

Say Skittles are produced by one unit of high fructose corn syrup and one bag. For Twizzlers you need one unit of red dye and one bag. Each bag of Skittles sells for \$2 and each bag of Twizzlers sells for \$3. You have 400 units of high fructose corn syrup, 500 units of red dye, and 700 bags available. What is the maximum profit you can achieve?

The solution to the problem is as follows:

We know that Twizzlers make use more money, so we want to make as many Twizzlers as possible. Thus, we make 500 bags of Twizzlers and 200 bags of Skittles for a profit of \$1900.

However, we can understand this problem in terms of variables and inequalities. We want to create an objective function that represents total profit. We have our variables s, t, where s represents the number of bags of Skittles we make and t represents the number of bags of Twizzlers we make. We have the inequalities $s \leq 400$, $t \leq 500$, $s + t \leq 700$, and $s, t \geq 0$

So, we want to maximize the function $2s + 3t$ and comply with the restrictions. In order to do this, we can let s and t be axes of a plane. If we graph our inequalities, we can visually represent the pairs of s and t's that comply with our restrictions. Dylan then explained that even larger systems, with a multitude of variables, could be, be represented geometrically and cut of regions in higher dimensions. The vertices of these objects that are created represent the possible values of the optimization. We (of course) didn't prove this.

An extension question that was posed was about the change in profit when our supply changed. If there is one more unit of red dye, or if there is one more unit of high fructose corn syrup, or if there is one more bag; how will the strategy change and what will the maximum possible profit be?

Then, Dylan introduced the idea of duality. Duality states that for every linear program with k variables and l constraints, there is a counterpart system with l variables and k constraints that represents the same problem. For our primal question of the changes in profit when the supply changes, we get the answer $+0$ profit change for one more high fructose corn syrup, $+1$ profit change for one more red dye, and $+2$ for one more bag. Our dual question would to minimize $400x + 500y + 700z$, where $x + z \geq 2$, $y + z \geq 3$, and $x, y, z \geq 0$. This gives the solution set $(0, 1, 2)$. We spent the last moments trying to understand how the dual works and why the one presented by Dylan represents the same problem. Dylan closed of his talk by explaining the importance and beauty of linear programming and the geometric structures that could be used to represent optimization problems.