

U(t)-Mathazine

The

# CHANGE

issue

2021

SUMMER

ISSUE NUMBER 6



UNIVERSITY OF  
TORONTO  
SCARBOROUGH

CENTRE FOR TEACHING  
AND LEARNING

# U(t)-Mathazine

---

---

In the past two years, we have all experienced significant changes in our lives as a result of the pandemic. The team that produces this magazine has decided on the theme of "change" in order to link our articles with the current pandemic experience. We have selected the new name U(t)-Mathazine to reflect the fact that we now have more contributors from all three University of Toronto campuses. We have also redesigned the Magazine's style to create a better platform for communicating mathematical formulas. Just like the many lessons that we have learned during the pandemic, we hope that these changes will result in a more accessible and inspiring mathematics publication.

Zohreh Shahbazi- Editor in Chief

## Table of Contents

### [1] Perspective Change in Tiling by Zohreh Shahbazi

Zohreh Shahbazi is an Associate Professor, Teaching stream at the Department of Computer and Mathematical Sciences at the University of Toronto Scarborough.

### [2] Crunching the Numbers, Crushing the Virus: Statistics and the Fight Against COVID-19 by Olivia Rennie

Olivia Rennie is a medical student at the University of Toronto. Olivia has been a statistics teaching assistant since 2016.

### [3] Looking Beyond the Obvious by Manaal Hussain

Manaal Hussain is a Ph.D. Candidate in the Social Justice Program at the Ontario Institute for Studies in Education. Manaal has been a mathematics teaching assistant and course instructor since 2014.

### [4] Elliptic Curve Cryptography with a Side of Groups by August Lu

August Lu is a computer science and mathematics student at the University of Toronto Mississauga.

### [5] The Mathematics of Juggling by Parker Glynn-Adey

Parker Glynn-Adey is an Assistant Professor, Teaching stream at the Department of Computer and Mathematical Sciences at the University of Toronto Scarborough.

### [6] Russell's Paradox by Pourya Memarpanahi

Pourya Memarpanahi has been a teaching assistant in mathematics at the University of Toronto Scarborough since 2012.

## [7] Book Review - Cubed: The Puzzle Of Us All by Trevor Cameron

Trevor Cameron is an English as a Foreign Language teacher/tutor and UTSC alumnus.

## [8] COVID and Change by Lilaani Thangavadivelu

Lilaani Thangavadivelu is currently a third-year student majoring in Neuroscience and minoring in French and Applied Statistics at the University of Toronto.

## [9] Studying Mathematics During the Pandemic and Beyond by Veselin Jungic and Listiarini Listiarini

Veselin Jungic is a Teaching Professor in the Department of Mathematics at Simon Fraser University. He is a 3M National Teaching Fellow and a recipient of several teaching awards, including the Canadian Mathematical Society Teaching Award and the Pacific Institute for Mathematical Sciences Educational Award.

Listiarini Listiarini is an artist enrolled both in Computing Science (major) and Mathematics (minor) programs at Simon Fraser University.

## [10] Why am I Obsessed with Linear Algebra? by Akira Takaki

Akira Takaki is a mathematics and computer science student at the University of Toronto Mississauga.

---

### Perspective Change in Tiling

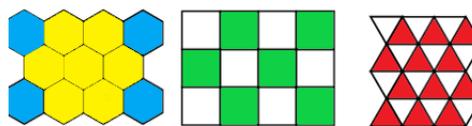
by ZOHREH SHAHBAZI

Imagine that you are supposed to create a carpet or use tiles to design the interior of a building. What would you do to create a beautiful design? If you were to create a sample pattern first and then repeat it to cover the entire space, you could save a significant amount of time. In addition, your design may look more pleasing at the end. Repeated patterns are abundant in nature — just think of mud flats, honeycombs, animal skins, molecules, leaves, spider webs, butterfly wings and desert sand.

In this article, we will briefly explore the mathematics behind repeated patterns.

Remember that a regular polygon is a polygon where all of its sides are of the same length, and all of its angles are of the same measure. In this note, a regular polygon with  $p$  equal sides is called a  $p$ -gon. In a regular tiling, we can fully cover an area with identical regular polygons (for example pentagons) such that there are no gaps and no overlaps in our

construction. There are just three regular tilings of a flat plane, namely the ones with equilateral triangles, squares, and hexagons (as shown in the image below).



A regular polygon tiles the plane if the following equation holds:

$$\frac{1}{p} + \frac{1}{q} = \frac{1}{2}.$$

Here  $p$  is the number of sides of each regular polygon and  $q$  is the number those polygons repeated at each vertex. For example with tiling with hexagons, we have  $1/6 + 1/3 = 1/2$ . The justification of this fact is that in the Euclidean plane the angle sum of a regular  $p$ -gon is  $(p - 2)\pi$  and thus all equal interior angles are equal

$$\frac{(p - 2)\pi}{p}.$$

At each vertex, we have  $q$  regular  $p$ -gons, thus

$$\left(\frac{p-2}{p}\right)\pi \cdot q = 2\pi.$$

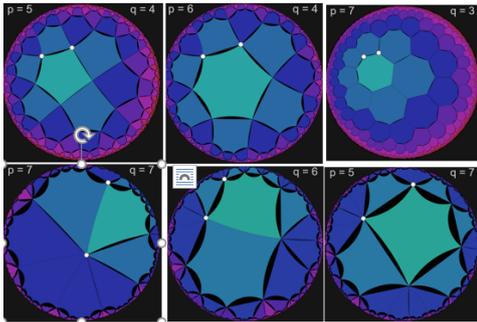
Now, we can simplify this last equation to obtain

$$\frac{1}{p} + \frac{1}{q} = \frac{1}{2}.$$

Let's change our perspective from the tiling of a flat plane to the tiling of a hyperbolic plane. The angle sum of a given triangle is less than  $\pi$  in a hyperbolic surface, so we can tile the hyperbolic plane with regular hyperbolic  $p$ -gons and  $q$  polygons at each vertex if

$$\frac{1}{p} + \frac{1}{q} < \frac{1}{2}.$$

There are infinitely many such  $p$  and  $q$  values that satisfy the equation. Therefore, there are infinitely many tilings for a hyperbolic surface. Several tilings of a hyperbolic surface are shown below. These images have been created by an online applet. The link of this applet is given in the reference section of this article.



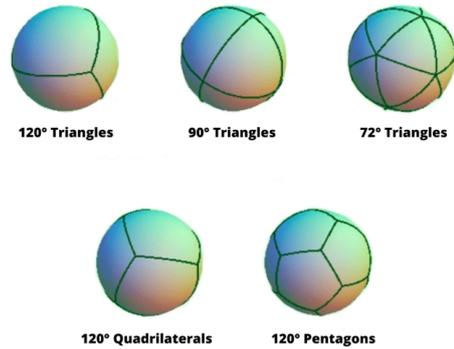
I used the same applet to tile an image of myself teaching spherical geometry (see below).



Let's change our viewpoint once again and look at tilings of a spherical plane. We can have a tile of a spherical surface if

$$\frac{1}{p} + \frac{1}{q} > \frac{1}{2}.$$

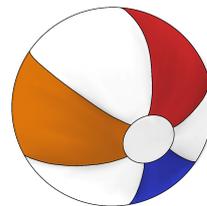
This is because the angle sum of a given spherical triangle is greater than  $\pi$ . Below are images of all possible tilings for a spherical surface with triangles, squares and pentagons:



These tilings are closely related to the five Platonic solids. If you flatten all of the polygon faces of any of these, you will end up with one of the five famous Platonic solids. Interestingly, on the sphere, we can have 2-gons which are also called lunas. In that case the inequality

$$\frac{1}{p} + \frac{1}{q} > \frac{1}{2}$$

is true for any natural number  $q$  which basically means that you can cover the surface of a sphere with any finite number of lunas. A beach ball is a good example of tiling a sphere with 6 lunas.



Considering fresh perspectives is often the source of a better and deeper understanding of any subject. This approach provides us with a natural assessment tool of our previous knowledge and helps us further develop our understanding. In particular, in mathematics, examining the various perspectives and aspects of a problem can help us to raise interesting questions which might lead us to new discoveries. For this reason, in this article, we looked at the concept of tiling in three different geometries to be able to understand the relationships better and enrich our understanding. This is very similar to the recent radical changes in our daily lives brought on by the pandemic, which have pushed us to expand our certain skills and explore avenues that we haven't explored before.

## References

<http://www.malinc.se/m/ImageTiling.php>

Baragar, A. (2001). *A Survey of Classical and Modern Geometries*. Prentice Hall.

Posamentier, Alfred S. (2012). *Advanced Euclidean Geometry*. John Wiley & Sons, INC.



Sourcing its data from a combination of specialized institutes, research publications, and statistical agencies, Our World in Data covers more than just COVID-19. Using the tools developed to explore issues as diverse as food distribution, deforestation, and global poverty, Roser's organization was in the perfect position to provide accurate, and freely available statistics on the pandemic. Users are even able to download complete datasets to run their own data analyses!

---

## Crunching the Numbers, Crushing the Virus: Statistics and the Fight Against COVID-19

by OLIVIA RENNIE

The COVID-19 pandemic has, without question, presented a unique set of challenges here in Canada and around the world. Not only has it been a devastating health emergency, but also an economic and social crisis, where livelihoods have been lost, families and friends separated, and people left yearning for activities once taken for granted. In spite of the immeasurable loss COVID has wrought, new insights have been birthed during this difficult time. Statistics have been essential since the start of this pandemic, gaining newfound respect from health professionals, politicians, and everyday citizens alike. With all eyes on daily figures and trends, the study of statistics has been given a spotlight during COVID-19- a one that is unlikely to go out anytime soon. While it would be impossible for this article to cover all of the ways statistics have been put to use during COVID-19, several interesting examples will be highlighted here.

## Publicly Available Databases: Keeping the World Current

Each day, people from around the world search for updated statistics regarding case numbers, hospitalizations, deaths, and more recently, vaccinations. One website that has focused its efforts on providing relevant, accurate COVID-19 data is Our World in Data, an initiative started by Max Roser of Oxford University (Roser et al., 2020).

## Planning Ahead: Accurate Predictions from Trend Analyses

Beyond day-to-day COVID metrics, statistics have been (and will continue to be) essential for modelling future trends and preparing for what lies ahead. As countries around the world know all too well, COVID-19 is a highly contagious virus which has also proven to be exceedingly mutable. Given what we know at present, understanding the different scenarios that might play out is key to distributing resources and raising public awareness. These statistics have proven to be so important that researchers have put significant efforts into better understanding the trends, and how we can make more reliable predictions moving forward. One such paper, published in the International Journal of Health Sciences, explored statistical methods that can be used to improve decision making surrounding disease control (Ison, 2020). As the article points out, focusing on short-term trends such as daily case counts or hospitalizations can be highly misleading. In this publication, assessments of various statistical methods were conducted, including Spearman's rho, Mann-Whitney U tests, Mann-Kendal tests, and Augmented Dickey-Fuller tests. While data collection was restricted to the United States, the overall findings suggested (not surprisingly) that a combination of different statistical methods is important for accurately interpreting trend data and making predictions for the future. More than anything, it highlights the continued work that is necessary to understand these and

other statistical tools, in order to assess both short- and long-term patterns in our data - and ultimately, to use these insights to fight the global pandemic.

## Statistics at Ground-Zero: Analyzing Data from COVID-19 Patients

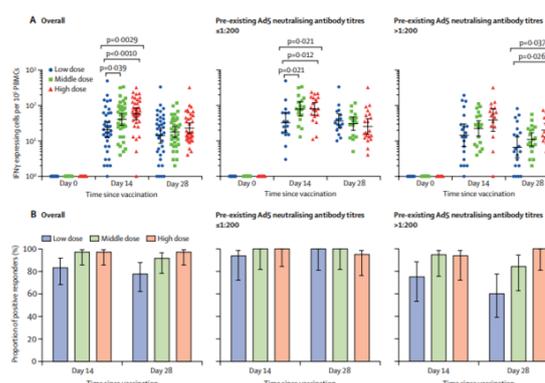
Not only are statistics essential for looking at big data related to larger-scale trends, but also in assessing patient outcomes and management within healthcare settings. However, just as with the trend analyses previously discussed, COVID-19 has taught us that we may need to re-examine the statistical tools used to analyze patient outcomes. Another recent publication in the journal *Clinical Epidemiology* outlined the pitfalls of various statistical methods in the context of the global pandemic (Wolkewitz et al., 2020). Many of these methods will be familiar to statisticians young and old alike, including Kaplan-Meier survival plots and Cox or logistic regression models. For instance, as this publication points out, in using standard Cox regression models for time-to-event analyses, competing events are often ignored. However, ignoring competing events can create issues, such as the death of a patient versus patients being discharged from hospital alive. For instance, looking at the interaction between competing events from a broader perspective can shed some light on the research question as a whole. In many cases, it can be tough to tease apart events that might seem to be unrelated, such as the aforementioned death versus hospital discharge example. However, research shows that in fact, while perhaps helping patients to heal, longer hospital stays also increase the risk of death. With respect to this specific example, Wolkewitz et al. suggest that Cause-specific Cox regression for both hospital mortality and hospital discharge helps avoid competing risk biases. Moreover, it also provides better understanding of the implications of treatment as a whole.

Looking at time-dependent predictors such as time to a patient requiring ventilation can also present statistical challenges and biases, as hazard ratios for a predictor and death tend to be underestimated. This is of serious concern, as it can lead to these predictors being missed or perhaps even considered beneficial. Ventilation may save the lives of some patients, but unfortunately, risk of death remains high (Luo et al., 2020). The impact of improperly applying statistical methods to pandemic data is not trivial. As articles are continually being published

about COVID-19, it is important for results to be reliable and accurate. Wolkewitz et al. put forth a concerning thought: that perhaps much of our epidemiological data on patient outcomes is fraught with errors, emphasizing that while statistics is of great value, it can also lead to biased conclusions with life-or-death consequences when misapplied.

## Statistics Shines Again: Making Sense of Vaccine Data

Perhaps the hottest topic of the present day is the arrival, distribution, and administration of the several COVID-19 vaccines now available. During the (still ongoing) vaccine development stage, vaccine efficacy has been a key area of interest as scientists around the world work tirelessly to develop new, safe and effective formulations. Here, as with everywhere else that data is captured, statistics bring meaning to the numbers. In the case of vaccines, assessing safety and efficacy is not as simple as just having a control and treatment group, and eyeballing differences on the page. Rigorous statistical methods must be utilized to verify that the benefit for those vaccinated is not simply due to chance. To get accurate results, large sample sizes must be used — ideally, samples that are representative of the population itself. Statistics are also essential in visualizing and communicating results to others, as can be seen by this set of figures from an early vaccine trial, published in *The Lancet* in June 2020 (Zhu et al., 2020).



Statistics also came into play during the early days of vaccine development, as researchers tried to think creatively about new trial designs that could be implemented, and which statistical methods (if any) would be appropriate for analyzing such data. As just one example, in an article originally published in 2020, different setups for vaccine trials were explored, such as 'efficacy trials,' and 'ring vaccination trials' (Jiang, Wang & Xia, 2020). Given

the state of emergency COVID-19 has created, developing and assessing vaccines as quickly as possible — while not cutting any corners in safety — was a challenge for all involved. As will be familiar to even introductory statistics students, basic principles of study designs must be considered, such as controlling for Type I Errors, using double- or single-blind techniques, and applying statistical methods that produce unbiased estimates. Clearly, it would be a waste of time and energy to widely administer a vaccine that was found to be ‘effective’ in a study purely due to random chance. Statistics come to the rescue again to help us feel confident in the efficacy of vaccines!

## Final Thoughts: The Power of Statistics in a Time Like No Other

This year has certainly been one of ups and downs. Each person has been challenged in their own ways, and together we continue to hope for the day when life will be ‘normal’ once again. Yet, this pandemic has taught us more than how to wear a mask or stay six feet apart from others. It has taught us the importance of data, and how to use it to our advantage in the fight against COVID-19. Unlike the infamous Spanish Flu one hundred years ago, we now have novel ways not only of collecting and disseminating data at an unprecedented rate, but also analyzing it. As demonstrated here, statistics are powerful, but must be used thoughtfully in order to provide accurate interpretations of this vast amount of data. It is an exciting time for statisticians and mathematicians at all stages, from those just beginning their undergraduate degrees to those nearing the end of a fulfilling career. Above all else, one thing is for certain — COVID-19 will leave plenty of data to go around. More importantly, the insights made today will also be essential in guiding us out of this unprecedented time, and in preparing for future pandemics.

## References

- Ison, D. (2020). Statistical procedures for evaluating trends in coronavirus disease-19 cases in the United States. *International Journal of Health Sciences*, 14(5), 23-31.
- Jiang, Z., Wang, X., & Xia, J. (2021). Considerations on the clinical development of COVID-19 vaccine from trial design perspectives. *Human vaccines & immunotherapeutics*, 17(3), 656–660. <https://doi.org/10.1080/21645515.2020.1815489>

Max Roser, Hannah Ritchie, Esteban Ortiz-Ospina and Joe Hasell (2020) - “Coronavirus Pandemic (COVID-19)”. Published online at [OurWorldInData.org](https://ourworldindata.org/coronavirus). Retrieved from: [‘https://ourworldindata.org/coronavirus’](https://ourworldindata.org/coronavirus) [Online Resource].

Wolkewitz, M., Lambert, J., von Cube, M., Bugiera, L., Grodd, M., Hazard, D., White, N., Barnett, A., & Kaier, K. (2020). Statistical Analysis of Clinical COVID-19 Data: A Concise Overview of Lessons Learned, Common Errors and How to Avoid Them. *Clinical epidemiology*, 12, 925–928. <https://doi.org/10.2147/CLEP.S256735>

Zhu, F. C., Li, Y. H., Guan, X. H., Hou, L. H., Wang, W. J., Li, J. X., Wu, S. P., Wang, B. S., Wang, Z., Wang, L., Jia, S. Y., Jiang, H. D., Wang, L., Jiang, T., Hu, Y., Gou, J. B., Xu, S. B., Xu, J. J., Wang, X. W., Wang, W., ... Chen, W. (2020). Safety, tolerability, and immunogenicity of a recombinant adenovirus type-5 vectored COVID-19 vaccine: a dose-escalation, open-label, non-randomised, first-in- human trial. *Lancet* (London, England), 395(10240), 1845–1854. [https://doi.org/10.1016/S0140-6736\(20\)31208-3](https://doi.org/10.1016/S0140-6736(20)31208-3)

---

## Looking Beyond the Obvious

by MANAAL HUSSAIN

Higher education institutions are meant to breed, train, and produce critical thinkers; the leaders of tomorrow. While we can take pride in equipping them with the academic knowledge, instil in them the importance of research development and synthesis, and prepare them to take on challenges that don’t even exist today, I cannot help but wonder if this is enough? Are we producing graduates who are fully capable of critically examining and challenging narratives, understanding how these narratives continue to position certain groups as inferior, and reshaping the narratives to level the playing field?

Reflecting back on my journey as a young person of colour imagining an undergraduate career in mathematics, I remember reading a lot of reports that flagged the persistent underperformance of certain equity seeking groups. This was particularly concerning to me as I had recently migrated to Canada; I was already disadvantaged as my curriculum, regardless of the scholarship that was awarded to me

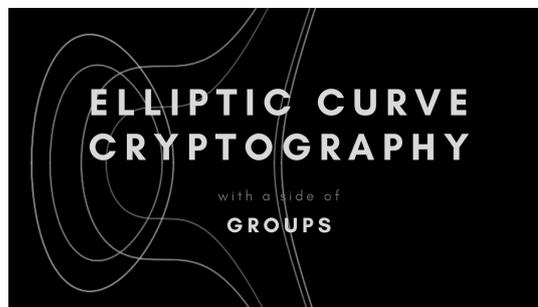
because of my high grades, was deemed to be “inferior”. Combine this with the fact that I had failed my diagnostic test – a test assigned to all students in week 1 of classes to assess their standing – I had no chance. Could it really be that I suddenly wasn’t good enough, and that my prior academic background held no credibility? Let’s pose the same question in another context – Imagine that you aspire to be able to win a game. It is crucial that you understand the rules first. You decide to spend hours learning the rules of the game. You find out on your day off that the game is to be played in a different language. You fail to translate the rules well, and end up losing the game. Would you say that you lost because you didn’t understand the game? Or because you didn’t understand the tool (i.e. language) that was used to deliver the learning (i.e. game).

This is a part of a bigger conversation that is oftentimes missing in STEM fields. Very rarely are our racialized identities and varied experiences acknowledged. Very rarely do these classrooms focus on creating equitable spaces. Very rarely is a culturally responsible and responsive pedagogy assumed in these spaces. Of the multiple identities a student brings with them to the classroom, the only identity that is acknowledged is that of being a student. Nothing more. A student might be battling an array of emotions because of how their community was targeted in recent times, but the only emotion they are to bring to these classrooms is that of a detached individual. While I can appreciate that these dialogues are easy to curate in the world of humanities and social sciences, it is unimaginable to suggest that STEM fields offer absolutely no space for such conversations to take place.

To my fellow teachers – explore ways in which equity-based pedagogy can be embedded into your curriculum. Explore assessments that leverage multiple competencies, and affirms learners’ identities. Challenge dominant narratives and spaces of marginality. Finally, equip your students to identify their privilege and place in society, and teach them how to be an ally to those in need. To my fellow students, the leaders of tomorrow – engage in equity-centered learning on your own. Develop an awareness of the various systemic inequalities at play, and how they might be acting as a barrier for some. Be an ally in the fight against racism – and other isms and phobias. Create a better society than the one you inherited.

## Elliptic Curve Cryptography with a Side of Groups

by AUGUST LU



### Some Background and Motivation

RSA, named after its inventors Rivest, Shamir, and Adleman, is one of the oldest algorithms in cryptography—the science of secure data transmission. This otherwise complicated cryptosystem can be summarized in a sentence for our purposes:

*It is hard to factor a large integer into prime numbers.*

We say it’s a *hard* problem in the computational sense. Crudely speaking, this means that there’s no known algorithm which can consistently do this in reasonable time on a classical computer. In the context of cryptography, this is exactly the type of situation we’d like to be in. Computationally-expensive problems make secure communication a reality, and, as we are about to find out, they appear in various forms.

The industry-standard RSA boasts a lifespan of nearly half a century, so one would naturally wonder why other cryptographic systems—such as elliptic curve cryptography—ever came to fruition.

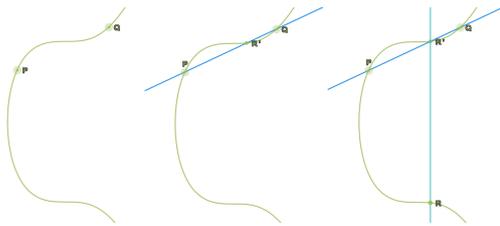
The study of elliptic curves far predates cryptography, but at present, these objects take on quite an applied role. In the same vein as RSA, **elliptic curve cryptography (ECC)** is a variation of public-key encryption which is shockingly, built on elliptic curves. One notable usage of ECC today is in cryptocurrencies like Bitcoin and Ethereum. Its considerably smaller key sizes, which don’t detract from the security, make it a highly appealing alternative to RSA when processing power and storage are limited. But all this talk dances around questions at the heart of the subject: what is an elliptic curve? What is the equivalent hard problem for ECC? How can

we send secret messages with it? We hope to untangle just some of the concepts that govern ECC.

Our definition of addition needs to be fleshed out a bit. What if  $P = -Q$ ? How do we compute  $P + Q$  here? In our case, the identity element is denoted by the symbol  $\infty$ , representing a point "at infinity".

## The Group Structure of Points

Below is a continuous version of a special curve named *secp256k1*, the one used in Bitcoin. It's given by the equation  $y^2 = x^3 + 7$ . Satoshi Nakamoto, the pseudonymous creator, chose this for "no particular reason."



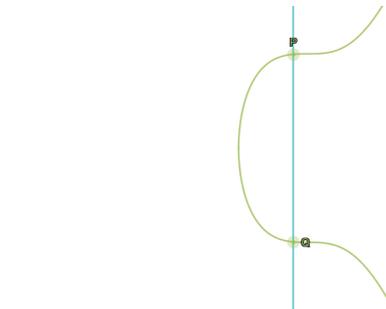
Let's geometrically define the addition of two points on a curve  $E$  as follows.

1. If  $P, Q$  are points on  $E$ , draw a line through  $P$  and  $Q$ . The point at which the line intersects  $E$  will be labelled  $R'$ .
2. Draw a vertical line through  $R'$ . We say  $P + Q = R$  where  $R$  is the point obtained from the intersection of the vertical line through  $R'$  with  $E$ .

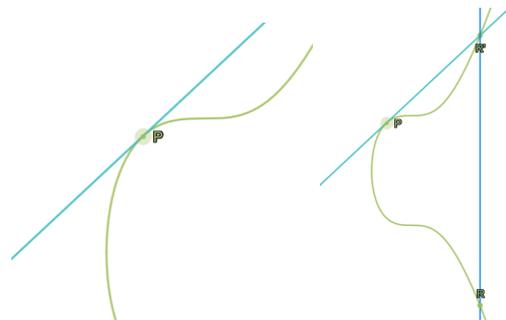
It turns out that the points of  $E$  form an abelian (i.e. commutative) group with respect to addition. Like a field, a group is an algebraic structure, albeit with significantly fewer restrictions. The study of groups is playful and vibrant, for there is an endless variety of examples arising from this lenience.

**Definition 1** Let  $G$  be a set endowed with a binary operation  $+$ . We say  $(G, +)$  is a **group** if it satisfies the following **group axioms**:

1. **Associativity.** For all  $a, b, c \in G$ ,  $(a + b) + c = a + (b + c)$ .
2. **Existence of an identity element.** There exists an element  $e \in G$  such that, for all  $a \in G$ ,  $e + a = a$  and  $a + e = a$ . When the operation is addition, we can think of this as the "zero" of the group, as we are hopefully familiar with the notion that adding zero to numbers gives the same number back.
3. **Existence of inverses.** For all  $a \in G$ , there exists an element  $b \in G$  such that  $a + b = e$  and  $b + a = e$ . This element  $b$  is usually denoted  $-a$ .



It doesn't tend well to geometric intuition, but  $P + Q = \infty$  by assumption. What about the case where we try to add  $P$  to itself?



The line passing through  $P$  is a tangent line, and now it's business as usual; our protocol for adding points works.

We can actually keep adding  $P$  to itself repeatedly with the same procedure. If we do this  $n$  times, denote this by  $nP$  for convenience. We will call this process **scalar multiplication**.

## Discrete Logarithm

At the beginning, we mentioned in passing the notion of a hard problem. In RSA, the time-consuming problem is factoring large integers into primes. It is here that we present the backbone of ECC—the discrete logarithm.

**Definition 2 (Discrete logarithm problem)**

Given two points  $P, Q$  on a curve, find  $k \in \mathbb{Z}$  so that  $Q = kP$ .

It may be surprising that this process can get extremely time-consuming for large values, so much so that it may surpass the universe's lifetime. Like RSA, there is no known algorithm that can solve this in polynomial time on a classical computer. To

calculate  $Q$  from  $kP$  is fast, since it's scalar multiplication, but to find  $k$  from  $Q$  and  $P$  is tedious, since it's the discrete logarithm. *It is precisely this that makes ECC secure.*

4. Leia computes  $S_L = k_L Q_V$  and Vraj computes  $S_V = k_V Q_L$ . As it turns out,  $S_L$  and  $S_V$  are actually the same.

$$S_L = k_L Q_V = k_L (k_V P) = k_V (k_L P) = k_V Q_L = S_V$$

## Diffie-Hellman-Merkle Key Exchange for Elliptic Curves

Consider the following allegorical scenario, used to illustrate key exchange between two parties at a high level.

Leia and Vraj want to gossip about their rival Imad using Biscord, a popular online messaging platform. Unbeknownst to them, Imad was recently promoted to head of operations at Brogers, their local internet service provider, and he is more eager than ever to violate the organization's code of ethics. How might the two exchange their secret texts over the application without fearing that a malicious actor at Brogers—perhaps Imad—might see them? The exchange of secret information requires these parameters:

- the prime  $p$  where the elliptic curve is defined over  $\mathbb{Z}_p$  (in practice, the ECC's curves are defined over a finite field like the integers mod  $p$  instead of  $\mathbb{R}$ )\*
- a point  $P$  on the elliptic curve which generates\* the group

The idea goes like this.

1. Leia and Vraj each generate a private key  $k_L$  and  $k_V$  respectively, where  $k_L, k_V$  are integers less than or equal to the cardinality of the group. No one is to know  $k_L$  except for Leia, and equivalently for Vraj.
2. They then generate public keys  $Q_L$  and  $Q_V$ . Given the shared generator point  $P$  of the subgroup (since they're using the same curve), Leia computes  $Q_L = k_L P$  and Vraj computes  $Q_V = k_V P$ . The names private and public key should be evocative of their visibility to third parties. Here's where we're at currently:

Key	Leia	Vraj
Private	$k_L$	$k_V$
Public	$Q_L = k_L P$	$Q_V = k_V P$

3. Leia and Vraj give each other their public keys  $Q_L$  and  $Q_V$ . It doesn't matter if Imad can see this.

Since they both share a common number, it can be used as a secret between them. It would not be possible for Imad to figure this out.  $S_L, S_V$  can now be used as the encryption key in something like a symmetric-key cipher for sending messages. Finding  $Q$  from  $k$  and  $P$  is easy (scalar multiplication), but finding  $k$  from  $Q$  and  $P$  is hard (discrete logarithm problem). This means that an outsider like Imad viewing the transmission will struggle to obtain the private key from information that may be public (the public keys  $Q$  and generator point  $P$ ). By "struggle", we of course mean by the standards of modern supercomputers.

\* *The technicalities of this are beyond the scope of the article. If it interests you, a more detailed explanation can be found here: <https://bit.ly/2Uv4swL>*

## References

El Housni, Y. (2018). *Introduction to the Mathematical Foundations of Elliptic Curve Cryptography*. HAL.hal-01914807

Koncovy, J. (2014). *Applications of Elliptic Curves Over Finite Fields*. [Honours project]. University of New Brunswick.

---

## The Mathematics of Juggling

by PARKER GLYNN-ADEY

## Introduction

Mathematics can appear in the most unlikely places; it doesn't always happen in a lecture hall. You might see a bit of mathematics performed at a circus if you look carefully enough. In this short note, we will explore the mathematics of juggling. Ronald Graham, a mathematical pioneer and expert juggler once said: "Juggling is sometimes called the art of controlling patterns, controlling patterns in time and space. Math is sometimes called the science of patterns."

## Throw Height

To explain how juggling works, we need to determine some features of juggling trajectories. In particular, we must know how high to throw the balls so that they land on schedule. Let us introduce a function  $h(t)$  to measure the height of the ball as a function of time measured in beats. The condition that the ball be thrown on beat zero, and land on beat  $n$ , can be re-written as  $h(0) = h(n) = 0$ . To determine the rest of the trajectory, we need to account for the influence of gravity. Ever since Newton saw an apple fall outside his mother's house, and observed that the same force was pulling the moon towards the Earth, mathematicians have modelled gravity as constant downward acceleration. As acceleration is the second derivative of position, we write the influence of gravity as a statement about the second derivative of  $h(t)$ .

We are looking to determine the maximum of a height function  $h(t)$  such that  $h''(t) = -G$  for a gravitational constant  $G > 0$ . Integration gives:

$$h'(t) = \int h''(t)dt = \int -Gdt = -Gt + C_1 \text{ (Eq. 1)}$$

and integrating again we get:

$$h(t) = \int (-Gt + C_1)dt = -\frac{G}{2}t^2 + C_1t + C_2 \text{ (Eq. 2)}$$

And now we must determine the values of the constants of integration  $C_1$  and  $C_2$ . The ball initially begins at height zero. So, we have the equation:  $0 = h(0) = C_2$ . Substituting this in to Equation 2 gives:  $h(t) = -\frac{G}{2}t^2 + C_1t$ . Our other condition on throw height is that the ball must land on the  $n$ th beat. Using the fact that  $h(n) = 0$  we get:

$$h(n) = -\frac{G}{2}n^2 + C_1n = n(-\frac{G}{2}n + C_1) = 0 \text{ (Eq. 3)}$$

Thus, solving for  $C_1$ , we obtain  $C_1 = n\frac{G}{2}$ . This tells us that our parabola must be

$$h(t) = -\frac{G}{2}t^2 + \frac{nG}{2}t \text{ (Eq. 4)}$$

This equation models the trajectory of a ball that starts at height zero and returns to height zero at time  $n$  beats. In mathematical physics, it is common to pick units that make formulas look nice. In this case, it is helpful to pick  $G = 2$ . We get the following parabola:

$$h(t) = -t^2 + nt \text{ (Eq. 5)}$$

To determine the maximum height of the ball, we optimize the function  $h(t)$  from Equation 5. Next,

we work backwards and take some derivatives. We have  $h'(t) = -2t + n$  and thus  $h'(t) = 0$  when  $t = \frac{n}{2}$ ; that is, the ball reaches its maximum height at halfway through its trajectory. Next, we can answer a fundamental question about juggling: In order for a ball to land at  $t = n$ , how high do we have to throw it? Using the parabola we calculated, we must throw the ball to height:

$$h(\frac{n}{2}) = -(\frac{n}{2})^2 + n(\frac{n}{2}) = \frac{3}{4}n^2 \text{ (Eq. 6)}$$

This means that the throw heights grow quadratically in  $n$ . If you to throw a ball so that it lands five beats later, you must throw it much higher than if you want it to land three beats later. How much higher? Well, using Equation 6, we can calculate:

$$\frac{h(\frac{5}{2})}{h(\frac{3}{2})} = \frac{\frac{3}{4}5^2}{\frac{3}{4}3^2} \approx 277\%$$

## Siteswap

We turn our attention to what patterns of heights are compatible when juggling. Suppose that we throw a ball to arrive three beats later. We can keep on throwing and catching the ball, with a nice even rhythm, and we would obtain:

X   -   -   X   -   -   X   -   -  
3            3            3

The Xs signify that we are holding a ball, and the blanks signify that we are not holding a ball. If we pay attention to the gaps in the sequence, then it is clear that we can add in another ball in between these beats:

X   Y   -   X   Y   -   X   Y   -  
3   3            3   3            3   3

There is one last set of evenly space gaps where we could place a ball:

X   Y   Z   X   Y   Z   X   Y   Z  
3   3   3   3   3   3   3   3   3

To describe this juggling pattern, we can say that we throw "3" on each beat. Thus, the pattern is called 3. This is the standard way that most people first learn to juggle, and it is called the "three ball cascade".

This notation for juggling patterns, called Siteswap notation, describes a juggling pattern as a list of durations measured in beats. It was discovered by many independent groups of jugglers in the late 1980s. Once jugglers had a system for writing down

juggling patterns, they were able to creatively explore the possibilities it enabled. The invention of Siteswap notation created an explosion of new and exotic juggling patterns. To get a sense of how the system works, we'll explain the first pattern discovered with this new notation.

Suppose that we throw a ball for a duration of four beats.

$$\begin{array}{cccccccc} X & & & & X & & & \\ 4 & & & & 4 & & & \end{array}$$

We could follow this with another throw for a duration of four beats.

$$\begin{array}{cccccccc} X & Y & & & X & Y & & \\ 4 & 4 & & & 4 & 4 & & \end{array}$$

Note that there is a small gap between the first XY and the second XY. Prior to the invention of Siteswap notation, no one noticed that you could insert a small quick throw of duration one in between these two groups; this means that we can throw a ball Z so that it lands one beat later.

$$\begin{array}{cccccccc} X & Y & Z & Z & X & Y & & \\ 4 & 4 & 1 & & 4 & 4 & & \end{array}$$

This creates the juggling pattern 441. This pattern, was one of the first genuinely new patterns discovered by mathematician jugglers, and is called 441 because the balls are thrown so that they land "four beats later, four beats later, one beat later" If we continue the pattern in this fashion, we get:

$$\begin{array}{cccccccc} X & Y & Z & Z & X & Y & Y & Z \\ 4 & 4 & 1 & 4 & 4 & 1 & & \end{array}$$

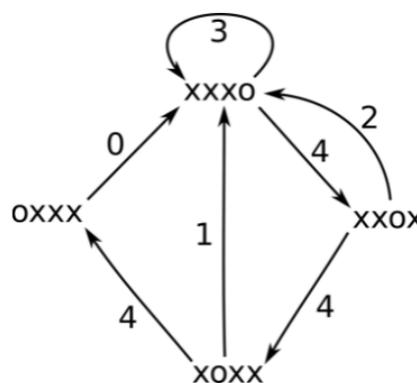
## States

So, thinking mathematically, we can ask: "What juggling patterns are possible?" The existence of the pattern 441 came as a surprise to many jugglers when it was first discovered. What other patterns could be lurking in the numbers?

Let's assume that we're going to juggle three balls, and that the highest possible throw will land four beats later. (This is a simplifying assumption, we could theoretically investigate juggling a hundred balls up to a thousand beats but nobody would be able to juggle them in real life.) If we're only throwing balls which land at most four beats later, then we only need to focus on any window of four beats. Since there are three balls, we must assign three balls to the four beats. This can be done in four ways:

$$\begin{array}{cccc} X & X & X & - \\ X & X & - & X \\ X & - & X & X \\ - & X & X & X \end{array}$$

We call these juggling states. They record when balls will land. To throw a ball, we advance time by one beat, and place the ball in the spot where it lands. For example, if we are in juggling state XYZ - and throw a ball to land four beats later then we obtain the state YZ - X. The first ball was thrown to the fourth beat. This framework allows us to construct a juggling state graph. There is an edge labelled k from state S to state T if T is the result of throwing a ball k beats when in state S.



Closed paths on this graph correspond to possible juggling sequences. The loop at the top is the standard cascade 3. If we follow the boundary of the triangle on the right hand side, we get the juggling pattern 441.

## Conclusion

In this rapid tour of juggling, we've seen calculus and a little bit of discrete mathematics. The mathematics of juggling is a surprisingly rich subject, with lots of discoveries still waiting to be uncovered. If you're eager to start experimenting, or to try out juggling, we encourage you to look at the following resources.

## References

Wall, T. (2020). *Juggling: What it is and how to do it*. Finnigan, D. (1987). *The Complete Juggler*.

## Russell's Paradox

by POURYA MEMARPANAHI

In this article, we will be exploring the **axioms of set theory**. It is known as “ZFC”, an abbreviation for “Zermelo–Fraenkel Set Theory with Axiom of Choice.” ZFC consists of 9 axioms. We will introduce six of them in this article. We will also deduce the existence of various types of infinities; more specifically the existence of larger and larger infinities. In future issues of U(t)-Mathazine, we will introduce the rest of the “ZFC” axioms with the ultimate goal for investigating the so called “Continuum Hypothesis.”

The foundation of our Mathematical World started off with sets and our studies of sets. Interestingly enough, it began with a set with no membership, which we call the “Null Set”. It is a set containing no elements, and it is denoted as  $\emptyset$ . Using that emptiness, we can actually construct another set, a set containing the null set as an element. Let us call it  $1 := \{\emptyset\}$ . We can keep on constructing more sets,  $2 := \{\emptyset, \{\emptyset\}\}$ , and we can keep on going,  $3 := \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}$ ... However, you should ask yourself, how did we get from 0 to 1? and then from 1 to 2? Well, we used one of the axioms of ZFC, “Axiom of Pairing.” What happened was we paired two sets, the set 0 and the set 1. So, our set 2 has two elements in it; the null set, and the set containing the null set as an element.

Let us introduce the **axiom of pairing**:

$$\forall x \forall y \exists z \ni: (x \in z \wedge y \in z)$$

That sequence of quantifiers can be read as for any set  $x$  for any set  $y$ , there is another set  $z$ , such that  $x$  and  $y$  are both elements of the set  $z$ . So, there is a set that contains both  $x$  and  $y$  as elements

Another axiom of ZFC, which I would like to introduce to you is the **axiom of union**:

$$\forall x \exists u \ni: (y \in a \wedge a \in x) \rightarrow y \in u$$

As a matter of fact, this axiom asserts a lot more than the existence of the union; it states that given any set  $x$ , there is another set  $u$ , such that  $u$  contains the elements of elements of  $x$ . Let us denote our set  $u$  by  $\cup x$ . This notation might make things easier for you to comprehend. Let us be more explicit. Consider the following example:  $x = \{2, \{4, 5\}\}$  then  $\cup x = \{\emptyset, 1, 4, 5\}$ . You should ask yourselves, what were the comprising elements of our set 2? Also, remember that  $\cup x$  can contain more elements! The quantifier stated there is a set! Note,

that given any set  $x$ , its elements are also sets themselves. These sets are called “hereditary sets”.

Another important axiom of ZFC for the purpose of this article is the **power set axiom**:

$$\forall x \exists y \ni: \forall a \in y (b \in a) \rightarrow b \in x$$

This axiom states that given any set  $x$  there is another set which consists of subsets of the set  $x$ . Let us denote that particular set as  $\mathcal{P}(x)$ .

There are 7 more axioms remaining if we acknowledge the existence of the empty set as our first axiom of ZFC. **Well-foundedness or axiom of regularity** is:

$$\forall x \neq \emptyset \exists a \in x \ni: (\forall b \in x, b \notin x)$$

or equivalently

$$\forall x \neq \emptyset \exists a \in x \ni: (x \cap a = \emptyset)$$

It basically deduces that every nonempty set has a minimal element with respect to  $\in$ -relation. Note that the above statement also implies that no set is an element of itself! The next mathematical notion which should come into mind once we have some sets to work with, is the idea of its *size*- basically the number of its elements. We call this the *cardinality*, and we denote it as  $|x|$ . If  $x$  contains finitely many elements, then we say its cardinality is finite and it is equal to some natural number  $n$ . This might not be very interesting. Interesting questions arise when we have a set which consists of infinitely many points. At this point we invoke another ZFC axiom called the **axiom of infinity** which asserts the existence of an infinite set.

$$\exists x \ni: (\emptyset \in x \wedge \forall a \in x) \rightarrow a \cup \{a\} \in x$$

It basically depicts that given any element in our set  $x$ , its immediate successor is also in that set. Note that we could not have concluded the existence of such a set using the previously mentioned axioms! Let us denote this set as “ $\omega$ ”. As an example, if  $2 \in \omega \rightarrow 3 \in \omega$ . Let us recall how we constructed 3. It was  $3 = 2 \cup \{2\}$ . 3 is the immediate successor of 2. Think of this set as the set of natural numbers along with zero.

Intuitively, it is an infinite set of the smallest size in the class of infinite sets. Galileo illustrated how there are infinities bigger than a given infinity. Draw a circle, he said, and draw infinitely many lines from the center, reaching the circumference of the circle. Now draw a bigger circle encompassing the given circle. Extend those infinitely many lines to reach the outer circle’s circumference. As

we are extending the lines, we are creating gaps in between, and now we can insert more lines in between and thereof, creating a “larger” infinity. Let us actually see a proof of this fact, using the *ZFC Axioms* that we have introduced in this paper. Before we proceed with our proofs, let us first develop a mathematical notion of two sets having the same cardinality (size), and or bigger.

Two sets  $\mathbf{x}$  and  $\mathbf{y}$  have the same cardinality if there is a bijective function  $\phi : \mathbf{x} \rightarrow \mathbf{y}$ . A bijective function is a 1-1 (injective), and onto (surjective) function. This means

$$\forall b \in \mathbf{y} \exists! a \in \mathbf{x} \ni : \phi(a) = b.$$

This reads: given any element  $b$  in our co-domain, there is a unique pre-image,  $a$ , for  $b$  under our function  $\phi$ . We also say  $\mathbf{x}$  has a smaller cardinality than  $\mathbf{y}$ ,  $|\mathbf{x}| < |\mathbf{y}|$ , if there is an injective, but not a surjective function,  $\phi : \mathbf{x} \hookrightarrow \mathbf{y}$ . Alternatively, two sets  $\mathbf{x}$  and  $\mathbf{y}$  have the same cardinality if there is an injective function  $\rho_0$  from  $A$  into  $B$  and an injective function  $\rho_1$  from  $B$  into  $A$ . This is the so called “Cantor-Bernsteing Theorem.”

We are now ready to establish the existence of larger infinities using mathematical concepts. We will achieve this goal by showing that given any set  $\mathbf{x}$ , the cardinality of its power set  $\mathcal{P}(\mathbf{x})$  is always greater than the cardinality of  $\mathbf{x}$ . Let us proceed with our proofs. Take any arbitrary set  $\mathbf{x}$  and let its cardinality be donated by  $|\mathbf{x}|$  as usual. First note that there is always an injective function from  $\mathbf{x}$  to its  $\mathcal{P}(x)$ , simply map  $a \in \mathbf{x}$  to  $\{a\} \subset \mathbf{x}$ . Suppose on the contrary those two sets have the same size, and hence there is a surjective map  $\phi$  among those two sets. Ultimately we could enumerate all the elements of  $\mathcal{P}(x)$ , indexed by the elements of  $\mathbf{x}$  itself. So,

$$\mathcal{P}(\mathbf{x}) = \{a_x : x \in \mathbf{x}\}.$$

Define the following set  $\mathbf{b} = \{x \in \mathbf{x} : x \notin a_x\}$ . This is possible using the **comprehension axiom** of *ZFC* which states given any set  $\mathbf{x}$  and any formula  $\psi$ ,  $\{x \in \mathbf{x} : \psi(x)\}$  is also a set. Note that  $\psi(x)$  just means  $x$  satisfies our formula  $\psi$ . Since any subset of our set  $\mathbf{x}$  is enumerated by the elements of  $\mathbf{x}$ , there is an  $x_0 \in \mathbf{x}$  such that  $\mathbf{b} = a_{x_0}$ .

Here we can ask ourselves the following questions: Is  $x_0 \in a_{x_0}$ ? “or”  $x_0 \notin a_{x_0}$ ? We cannot have the former case. Why not? Well, if  $x_0 \in a_{x_0}$  then  $x_0$  cannot be an element of  $\mathbf{b}$ , since it does not satisfy the formula defining  $\mathbf{b}$ , so,  $x_0 \notin \mathbf{b} = a_{x_0}$ , and that is a contradiction with our original choice  $x_0 \in a_{x_0}$ . So, you might think that it should be the latter case,

right? Unfortunately, that case will lead us to a contradiction as well! If  $x_0 \notin a_{x_0}$ , then  $x_0 \in \mathbf{b} = a_{x_0}$ ! This is what it is called “*Russell’s Paradox*”. Hence we cannot enumerate the power set of any set by the elements of that set, implying the existence of larger cardinalities.

This brings us to the end of the first part of this article. We will scrutinize more in depth concepts in our next article, and build the foundation and framework to study “*Continuum Hypothesis*.”

---

## Book Review - Cubed: The Puzzle Of Us All

by TREVOR CAMERON

Ernő Rubik’s new book “Cubed: The Puzzle Of Us All” is a fairly scatterbrained compilation of loosely related musings that most readers will find approximately as interesting as they find the man himself. Although it’s a bit rough around the edges, this is perhaps for the best. It comes across as an honest (if perhaps guarded) portrait of the mind behind the Cube.

The book is a bit difficult to categorize. It isn’t exactly a memoir or autobiography in the traditional sense; if you’re hoping to learn more about Rubik as a person, you might find yourself disappointed. Autobiographically speaking, he keeps his cards fairly close to his chest. He sketches the basic schematic of his personal life as a professor of architecture, but keeps most of the finer details to himself. He goes into his upbringing and relationships with his (now deceased) parents a fair bit, but makes only passing reference to his own family—usually not even by name.

However, if you’re interested in his philosophies on life, or on his work, there’s plenty to sink your teeth into. Along with the history of the Cube, this is the meat and potatoes of the book. But it must be said that the book is more than a little disorganized. Rubik makes repeated reference to the fact that he “hate[s] to write”, and, well, it would appear that he hates to edit too. Although the events leading up to the advent of the Cube are sprinkled in in approximately chronological order, there is otherwise little in the way of discernible structure. Indeed, Rubik himself writes: “When I began this project, I was determined that the book not have an evident structure. I definitely didn’t want chapters and imagined it to have almost no beginning and

no end." The book is divided into six chapters, but as per Rubik's wishes, it's not entirely clear what divides one from another. Each chapter consists of a series of largely unconnected mini-essays, where Rubik muses on the nature of human curiosity, creativity, the connections between the arts and the sciences, and the universal appeal of puzzles (the book's subtitle is, after all, "The Puzzle Of Us All"). Structural quibbles aside, these bite-sized meditations are generally insightful, and likely worth the price of admission on their own for any prospective reader. The book's six chapters are bookended by a brief introduction from the perspective of the anthropomorphized Cube, as well as a post-script interview with both Rubik and the Cube. Although Rubik's own reflections on the book (which include the above quote) are quite interesting, the whole talking Cube thing comes across at best as silly. There may be the kernel of an interesting narrative device there, but as it is, it's a bit more like a segment from a children's puppet show.

As for who the book is for, I think a fairly wide variety of people might find something to enjoy, from casual former childhood Cubers to competitive Speedcubers, puzzle enthusiasts to math majors—the common denominator simply being an interest in Rubik or the Cube. But that's not to say that the book is only for hardened Cubers. Personally, I went into it more or less blind. I made a conscious decision not to get a Cube until after I finished this review, in order to be able to present the outsider's perspective (which, particularly as an English major, I certainly am). I've held a cube in my hands once or twice, but never owned or solved one. This is a bit odd in hindsight. I am passably familiar with a decent variety of puzzles, having had an uncle with a masters degree in pure math growing up who was always giving me puzzles and brain teasers for Christmases and birthdays, but somehow the Cube has nonetheless evaded me.

So if, like me, you don't have much or any experience with the Cube, this doesn't necessarily preclude you from reading the book (and even enjoying it). For the most part, it's written to be intelligible to the uninitiated, although there are some sections that seem to presuppose a great deal of puzzle-related knowledge. In particular, early on in the book, Rubik spends a good deal of page space discussing the various puzzles that inspired the Cube, rather matter-of-factly, and without a single diagram. You're probably going to want to have Google Images handy as you read. I know I did. The complete lack of visual aids throughout the book is particularly glaring, and perhaps even ironic, given

that Rubik often meditates on the limitations of language as a medium for communicating ideas. The only visual to be found is a small Cube in the bottom corner of each page by the page number, which will spin and solve itself if you flip through the pages (a rather nice touch).

All told, if you're interested in taking a glimpse at the rather eccentric mind of Ernő Rubik, you will most likely find what you're looking for here. The book may be a little bit all over the place, but its messiness lends it a certain charming authenticity. And for what it's worth, I've just ordered a cube of my own.

---

## COVID and Change

by LILAANI THANGAVADIVELU

I consider myself to be a part of the lucky group of first year students. Those who entered their first day of university classes in the fall of 2019 had the opportunity to experience many firsts in-person (ex. lectures, exams, between class breaks, meeting friends). When the pandemic hit and there were talks of switching university education to online, many felt nervous, but we were lucky enough to have had the privilege of experiencing at least some of first year in person. I know many people feel that COVID-19 has caused a lot of chaos, but for me, it has been my reason for change.

I thought high school was going to be my last time doing any math. My calculator was hidden in my backpack until I realized I still had one more math related course to complete for my Neuroscience major: Introduction to Statistics. I took a deep breath, rummaged through my bag to find my calculator, and walked into my then final math class ready to go, and to my surprise, it would turn out to be far from my last math class.

The word "Statistics" itself sounds tricky. Three t's three s's. On a good day, I would get confused with the spelling. Just imagine a stressful day! If you have had a poor experience learning math in the past, it seems dreadful having to pay for a course that you seem to have always struggled in. However, statistics is unique. It is the type of math that you can say is actually used in your everyday life. With some practice and a lot of help when in doubt, you can actually change your perspective on math.

I knew that I would have to start early on getting help. I invested in a textbook, only to realize my eyes were drooping by the end of the first paragraph. I struggled to keep up during the lectures and would get too nervous to ask questions. That is when I made the switch. I started looking into solving the professor's practice problems, spent many hours in the Math and Statistics Learning Centre, made a group of friends to bounce ideas off of whenever we were confused, and watched lecture recordings from the comfort of my own home. In fact, for the first time in my life I felt extremely elated when I began working on my biology lab report and understood the significance of the p-values in the study's results. Even when the pandemic started and we had to begin learning from home, it was very manageable to keep up with the work and feel accomplished. Statistics made sense.

I slowly started wondering: will this appreciation of statistics fade away after this course? I was still contemplating what I wanted to do. How could I, a person who came in for Neuroscience, be enjoying a statistics course? Did that mean I was heading down the wrong path? It was during this time when I was introduced to the Applied Statistics program. It opened up the possibility of pursuing both a science and applied statistics degree, without giving up either.

Now, at the end of my second year of university, I have had the opportunity to continue in my statistics journey while simultaneously pursuing my science courses. Although I had to make adjustments to my studying methods and reach out for help as needed, the statistics centre and the professors have been extremely compassionate and supportive. Choosing this program is one of the best decisions I have made in my undergrad experience. It has guided me toward many opportunities and potential postgraduate studies which combine my passions, such as epidemiology. Although I was initially apprehensive of making the jump, choosing to pursue an Applied Statistics minor reminded me that sometimes, change is good for you.

---

## Why Am I So Obsessed with Linear Algebra?

by AKIRA TAKAKI

Before I answer the question in the title, I'd like to talk about linear algebra as a whole. Linear algebra has a long rooted history in equations—*systems* of equations, in fact— that look a little like this:

$$\begin{aligned} 5x + 3y + 7z &= 8 \\ 9x + 20y + 8z &= 3 \\ 420x + 6y + 9z &= 1337 \end{aligned}$$

How would you even begin to solve this?

In my opinion, the huge change just comes with a shift in perspective. Instead of looking at this, consider it as a “matrix-vector” product, like this:

$$\begin{pmatrix} 5 & 3 & 7 \\ 9 & 20 & 8 \\ 420 & 6 & 9 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 8 \\ 3 \\ 1337 \end{pmatrix}$$

The way we define the multiplication between the matrix and the vector is exactly what you saw with the top three equations. In essence, we've changed nothing but the aesthetic of the equation.

However, doing it this way, pushes for a drastic change in perspective. If you now consider the “matrix” (3 by 3 looking object) and the “vector” (both 3 by 1 looking objects), you get a different kind of thinking.

For mathematicians, it's thinking of matrices like functions. Yeah, functions like  $f : x \mapsto x^3$ . Except, in this case, the inputs and outputs are vectors, which are these sorts of  $n$ -dimensional numbers. This change in thinking lets you think and ask of things like when is this function one-to-one (every output has a unique input) or when is this function onto (every output has at *least* one input)?

Before I get into that: already it can be overwhelming to have so many numbers and variables on screen. We're talking about one equation and there are already 12 numbers and 3 variables. That can get really messy, really quickly!

So our shift in perspective needs one more thing. We're going to call the matrix  $A$ , the input vector  $v$ , and the output vector  $b$ . Now our equation becomes:

$$Av = b$$

Much simpler, isn't it? The keen readers must be bewildered—how can we differentiate between numbers and vectors and matrices if they're all just letters? It's all about context—much like the English language itself. We use specific letters for specific things because it's very suggestive to the reader, and very helpful for people to follow along with what we're talking about.

In the context of linear algebra, lower case letters are usually vectors like  $u, v, w, x, y, z$  and constants (real numbers or complex numbers, whatever the situation calls for) are denoted with  $a, c, k$  but honestly, it's up to the writer, and they usually stick with one convention. Capital letters are almost always used for matrices.

Back to the system of equations.

$$\begin{aligned} 5x + 3y + 7z &= 8 \\ 9x + 20y + 8z &= 3 \\ 420x + 6y + 9z &= 1337 \end{aligned}$$

If you've studied a bit of vectors and systems of equations, you know that there are three possibilities.

- The equations have zero solutions.
- The equations have one (unique) solution.
- The equations have infinite solutions.

This might be confusing to think about, but the idea is that once you have more than one solution, you can do all sorts of rearrangements with your inputs to get infinitely many more. What does this correspond to in terms of function language? Well, we can talk about the whole set of vectors, and not just look at a particular one. If every vector  $b$  has a solution, that means  $A$  is onto. For a given vector  $b$ , if the solution to  $Av = b$  is unique, then  $A$  is one-to-one.

We actually phrase these things in terms of more complicated terms like linear independence and span, but I don't want to get into too much depth yet. So let's work with our matrix! Notice that we can rewrite the matrix product as follows:

$$\begin{pmatrix} 5 & 3 & 7 \\ 9 & 20 & 8 \\ 420 & 6 & 9 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = x \begin{pmatrix} 5 \\ 9 \\ 420 \end{pmatrix} + y \begin{pmatrix} 3 \\ 20 \\ 6 \end{pmatrix} + z \begin{pmatrix} 7 \\ 8 \\ 9 \end{pmatrix}$$

By varying  $x, y, z$ , we can get every possible output of this matrix. Now the question is, how can we write this in a simple way?

It's a matter of finding out which vectors are "redundant" in their information. In this case, there are none. (Showing this is outside the scope of this article, but you can take a class in linear algebra to find out.) The idea of redundancy looks like this:

$$\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \right\}$$

Clearly, the third vector doesn't help in giving any information, because we can create it from the other two. This is much more formalized in linear algebra proper, and it's really interesting.

With this equation:

$$\begin{pmatrix} 5 & 3 & 7 \\ 9 & 20 & 8 \\ 420 & 6 & 9 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = x \begin{pmatrix} 5 \\ 9 \\ 420 \end{pmatrix} + y \begin{pmatrix} 3 \\ 20 \\ 6 \end{pmatrix} + z \begin{pmatrix} 7 \\ 8 \\ 9 \end{pmatrix}$$

We can actually find that by varying  $x, y, z$ , not only can we get any vector in  $\mathbb{R}^3$ , they will all have unique solutions.

## Why Is Any of This Worth Taking an Entire Class Over?

Even if you think the above studies and going deeper might be of some interest - you have yet to see how wide-reaching linear algebra and it's studies go.

## Quantum Mechanics

The way electrons behave with orbitals, spins and the general information they possess—all this can be modelled very well by complex vectors, and concepts like *quantum entanglement* are just talking about the kind of *redundancy* of information in vectors we highlighted earlier. Heck, the notation is very suspiciously lifted from vectors:

$$\langle \phi | \varphi \rangle = \langle \phi, \varphi \rangle$$

where the left side is the bra-ket notation, and the right side is the inner product notation used in your second linear algebra class.

For example, the Hadamard transform  $H$  is literally a matrix, as follows:

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

## Economics

Suppose you want to find a way of changing your stocks based off of your returns, and you can find a relation between your stocks growing/decreasing from each other. It could look something like this, where  $G$  is the change in the GME stock and  $M$  is the change in the Microsoft stock.

$$M' = -2G + 0.5M$$

$$G' = G - M$$

Somehow you've reached back into the hands of linear algebra!

## Linear Regression

Finding the curve of best fit according to a model, or finding a bunch of continuous curves to fit (cubic spline kinda deal) involves a bunch of systems of equations—and again— that's just linear algebra.

Linear regression is important— it lets you predict things to come, or things that have happened in-between (like in a chemistry experiment and you have insufficient data for some time period).

## Machine Learning

In essence, what a lot of neural networks do, is take in an input vector, which could be a 256 by 256 im-

age, or even a video, comprising of 10000 frames of these images, which is still a vector, and use a bunch of linear algebra and calculus to figure out what to do. Here linear algebra here lets you gather data specific sections in the data set - for a data set of images of bees, you could be looking for the yellow and the black, and trying to remove the other components. It's all about the values in that matrix—you have to tweak them appropriately so that the right values get accentuated.

## Conclusion

I could go on and on about linear algebra, but there's no substitute for actually taking a linear algebra course. It's probably the one topic in math that you can see being used in many different places, and it's really cohesive in it's study! Everything in the first two linear algebra courses is interrelated (span, independence, injectivity, surjectivity, bases, invertibility, inner products), and it's kind of beautiful that it all works out. That's probably why I'm so obsessed with linear algebra. It appears everywhere and it's just a beautiful subject.

### Studying Mathematics During the Pandemic and Beyond

by VESELIN JUNGIC AND LISTIARINI LISTIARINI



Dream big - because anything is possible! Pictured here is an illustration of a mathematics student taking notes during a lecture - an image conceptualized by Professor Veselin Jungic of Simon Fraser University and his student Listiarini Listiarini. Look closely at the image and you'll notice that behind the

student is a photo of Professor Maryam Mirzakhani, the first (and only) woman and Iranian mathematician to be awarded the Fields Medal, the most prestigious award in mathematics. Throughout her life, Maryam pushed boundaries, and was known for her innovative ideas and relentless curiosity. Maryam was a professor at Stanford University up until she passed away from cancer at the age of 40. Despite the brevity of her life, Maryam's legacy lives on in the hearts and minds of students like the one shown here. So, believe in yourself and pursue your dreams! A career in mathematics and/or statistics is limitless, with countless opportunities to contribute meaningfully to the field and the world at large. What do you think about this image? What other elements of this image relate to your personal journey learning or teaching mathematics? Can you try to solve the following integral problem that appears on the student's tablet?

$$\int_0^{\pi/2} x \cos^{2n}(x) dx$$

You can send us your thoughts or the solution to this integral problem by **November 29, 2021**. Our email address is: [mathstats.utsc@utoronto.ca](mailto:mathstats.utsc@utoronto.ca).

## Call for Submissions

Have a topic in mathematics and/or statistics that you're passionate about? Want to have your voice heard? Then look no further, because this is your chance to contribute to the next edition of the U(t)-Mathazine! The process is simple: send us your articles or ideas by **November 29, 2021**. Articles should be a maximum of 3 single-spaced pages, including any figures. We welcome a variety of different submission types - standard text articles, illustrations, drawings, comics, creative writing, research, book reviews, etc. Have an idea but not sure where to start? Please get in touch, and we will be happy to help you with the writing and editing process. Articles and inquiries should be directed to our email address: [mathstats.utsc@utoronto.ca](mailto:mathstats.utsc@utoronto.ca)

We look forward to receiving your submissions!

**CONTRIBUTORS:**

Editor-In Chief & Designer: Zohreh Shahbazi

Editors: Parker Glynn-Adey & Olivia Rennie

Publishing Editor: Trevor Cameron

Communication Officer: Olivia Rennie

Special Contribution: Manaal Hussain

Cover Design: UTSC Printing Department