

*The Cute Goose honked
at you ferociously!



B! 2020

Ness	Paula	Jeff	Poo
HP 321	HP 113	HP 300	HP 251
PP 13	PP 200	PP 0	PP 50

mathASKS 143.5

FEATURING PROFESSOR DOUGLAS STEBILA

SUPERSINGULAR ISOGENY POST-QUANTUM CRYPTOGRAPHY: HOW DO WE PRONOUNCE YOUR LAST NAME?

stuh-BEEL-uh. But I've heard many variants.

VINCENT: THOUGHTS ON ONLINE PROCTORING SOFTWARE?

For a graduate exam of 3 students all of which were in town and had good Internet connections, I did online proctoring via Zoom where each student had a paper copy of the exam-hand delivered and then put their laptop across the room so we could watch their whole workspace. That worked. But for hundreds of undergrads spread around the world? I can't see it working. Not everyone has good Internet access. Not everyone has a laptop with a working webcam. People have technical failures. For MATH 239 online this term, we're having enough troubles getting students just to upload photos of their written solutions within the extra 1 hour time window we've added to the normal exam duration. (Please, please don't wait until the last 5 minutes to start taking pictures and uploading.) If you try to do online proctoring at scale, you need a way to accommodate technology failures, but any process for accommodating technology failures can equally be exploited for violating academic integrity. I can't see a way for us as instructors to distinguish the two cases. If we're in the unfortunate situation of having to deal with remote learning for the long-term, I think the only viable solutions are in-person exams in exam centres, or oral exams. (I'd be very interested in complementing written take-home exams with a 5–10 minute oral follow-up exam: “explain your solution to problem N.” But I'm teaching large classes so even 5-minute oral exams are beyond the resources we have right now.)

ROYAL NO.69 MILK TEA: WHAT'S THE HARDEST THING ABOUT TEACHING THIS TERM'S ONLINE VERSION OF MATH 239?

The hardest part for me has been a lack of connection with students. I find it much harder to get a sense of whether what we're doing is working for students. In-person lectures have real-time feedback, so you can adjust during the class and in subsequent lectures. But we're prepping videos a week or more in advance, so there's no scope for real-time adjustments. We do get a lot of posts on Piazza (more than 1800 so far and we've still got 3 weeks to go), but that medium is more limited. Compared with other core courses, MATH 239 is the start of a change in expectations: students are expected to work more independently to develop their own examples and be able to answer for themselves the question “is this proof correct?”; but it's very hard to communicate that change in expectations and for students to adapt to that with everything being unexpectedly remote.

TLLLOW PRINCESS: WHERE IS YOUR FAVOURITE TOILET ON CAMPUS?

I think the Math faculty's spa and hot springs resort has the nicest bathrooms.

CC: WHEN DO YOU THINK POST-QUANTUM CRYPTOGRAPHY WILL SEE WIDESPREAD ADOPTION? WHEN DO YOU THINK IT NEEDS TO?

I think there's good momentum right now from academia, government, and the top end of the tech industry. Assuming the NIST competition remains on track (see related question below), I think we'll see major tech vendors shipping post-quantum crypto in some parts of the Internet ecosystem within the next 2–3 years. But the problem is the long tail—for every Google or Microsoft or Apple that has the resources and expertise to properly implement and deploy these new algorithms, there are hundreds of companies that will struggle. Right now it's really important that vendors are building systems with agility: designed to be updated with new algorithms when they become available in the next 3–5 years.

QUANTUM PERSON: WHEN WILL NIST ROUND 3 START?

(For those who need some more context: The United States National Institute of Standards and Technology (NIST) standardizes cryptographic algorithms, and is currently running a public competition for standardizing post-quantum cryptography. The set of algorithms under consideration goes through several rounds of narrowing.)

NIST round 3 was announced on Wednesday July 22. UW researchers are involved in two round 3 finalists and two round 3 alternate candidates.

QUANTUM GOOSE: YOU HAVE A LIST OF COUNTRIES YOU'VE TRAVELLED TO ON YOUR HOME PAGE (www.douglas.stebila.ca). WHAT DID YOU ENJOY THE MOST ABOUT EACH?

When you're there, it's the sense of wonder from seeing new things and a different way of living (or realizing that it's in fact not so different). Afterwards, it's the feeling that these places are no longer abstract: when I read in the news about somewhere I've been, I can picture the streets I walked and the people I met, and that makes me care much more about what happens there.

CIX: WHAT IS YOUR FAVOURITE BOOK?

Besides *Protocols for Authentication and Key Establishment, Second Edition*, by Boyd, Mathuria, and Stebila, which makes an excellent birthday or Christmas gift and is available right now on Amazon.ca for just \$156.69? I read a lot of light sci-fi and fantasy. Some of my favourites are *Ender's Game*, the *His Dark Materials* trilogy, and the *Hyperion* cantos. And since we no longer have to be ashamed of reading fan fiction, *Harry Potter and the Methods of Rationality*: what if Harry was smart, and applied the scientific method to magic?

CLARIFIED: IN WHAT WAYS HAS UW CHANGED SINCE YOU WERE AN UNDERGRADUATE STUDENT? IN WHAT WAYS HAS IT STAYED THE SAME?

What's changed? So many new buildings on campus; and there were very few off-campus apartment towers. I think there were fewer geese back then; certainly there was no cult of Mr. Goose. Computer monitors are lighter now. (So much lighter. I remember lugging around a giant-for-the-time 17" CRT monitor weighing 40 pounds every time I moved for co-op.) We submitted paper resumes for co-op jobs into drop boxes in Needles Hall.

What's the same? Many of the math courses. (I kept all my notes from my undergrad, and the core courses still cover the nearly all the same material. I don't think they've gotten easier, if anything some of the core courses have more emphasis on proofs than when I went through.) Complaints about the co-op matching algorithm seem eternal.

MATHSOC PERSON: ANY INTERESTING STORIES FROM WHEN YOU WERE MATHSOC PRESIDENT?

In August 2002, UW announced that it would accept \$2.3 million from Microsoft for research and education initiatives, which included adopting C# in first-year ECE courses, and considering using C# in undergrad CS courses (<https://bulletin.uwaterloo.ca/2002/aug/15th.html>)—without any of this being approved by faculty academic councils or Senate. For some historical context, anti-Microsoft sentiment was at its high point: this came just one year after Microsoft had been convicted of abusing its Windows monopoly to advantage Internet Explorer over Netscape Navigator, and earlier that year Microsoft had lost a lawsuit against Sun Microsystems about breaking Java compatibility. At the time, C# was just a couple of years old, only ran on Windows, and was thought of by many as Microsoft's attempt at a "Java-killer." So there was the perception on campus (and among alumni) that UW had sold its curriculum to an evil corporation. We (MathSoc, Feds, student senators) very quickly set up meetings with then-UW-President David Johnston and the chair of CS, saying curriculum changes like this needed to be academic decisions through the standard university bodies with student representation. The CS faculty voted to not consider any new language for 6 months. If I recall correctly, UW signed a deal without money related to the C# provisions, and CS never adopted C# (but ECE did for a while).

BOLDBLAZER: WHAT PARTS OF THE OPTIMIZATION PART OF C&O ARE MOST APPLICABLE IN TERMS OF OPTIMIZING SPEEDRUNS OF VIDEO GAMES?

One of my former grad students apparently held some speedrun records in an old, obscure Super NES video game I'd never heard of (*Breath of Fire II*). So it seems to me that the most applicable part of C&O for optimizing speedruns of video games is having sufficiently many skilled graduate students with too much spare time.

GOD ⚡ PEED: IF YOU COULD MAKE EVERYONE FOLLOW ONE ONLINE SECURITY RULE, WHAT WOULD IT BE?

Can I pick three? Use a different password on every site. Don't open links or attachments in dodgy emails or downloads from dodgy sites. Keep your software up to date.

SANDWICH EXPERT: IS A HOT DOG A SANDWICH?

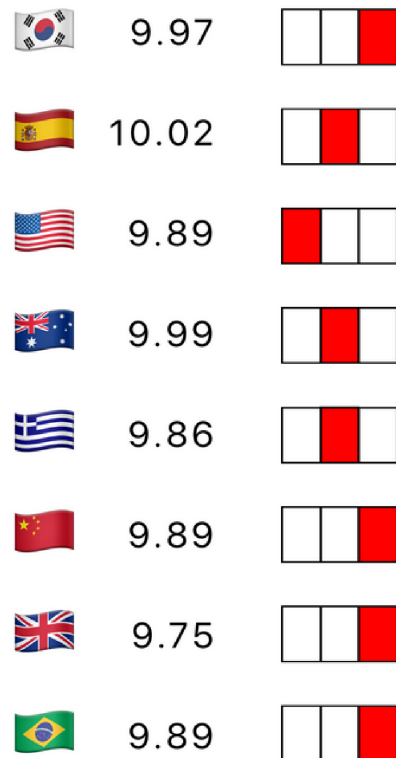
Nope. Most hot dogs are served without the bun being severed into two pieces. Separated top and bottom is the critical condition for me.

THE WEEKLY PUZZLE CHALLENGE — PUZZLE #3!

Get your thinking caps on, the Math Student Life Team in partnership with MathSoc present the Weekly Puzzle Challenge Here is this week's puzzle. For more details, the submissions form, and a list of rules visit <https://bit.ly/UWPUZZLE>. Each correct solution submitted before the deadline will give participants an entry into our prize raffle for a \$50 Amazon e-gift card (must be a registered UWaterloo Faculty of Math student to be eligible for the raffle).

Check out the puzzle here: <https://bit.ly/UWPUZZLE>.

Where did you run?



HASHING ALGORITHMS: THE TL;DR OF COMPUTERS

If you ever find yourself downloading something from the internet, sometimes you might notice that the website provides a “hash” of the file. This hash could look something like this:

```
b71e1220d212768c0637a7630f73386291c53f8d3f4dbfbf-
6dec44087f6af54 file.txt
```

If you found yourself wondering what this string of letters and numbers means, you're in the right place! Because I'm going to tell you about hashing algorithms.

A hash function is a one-way function that takes some data—some text, or a file, or really anything that can be expressed as a bunch of ones and zeros—as input and spits out a hash value corresponding to that data. The key here is *one-way*: generally speaking, you can't “undo” the hash function to get back the data you started with. Of course, if you're someone with a lot of money and/or GPU horsepower, these rules don't *necessarily* apply to you (Stevens et al. 2017), but I digress.

Hashing algorithms in common use, like MD5 and SHA256, generally have some cool properties:

- The hash is of a *fixed size*: for example, a SHA256 hash is exactly 256 bits (32 bytes) long, no matter how short or long the message is. You can write out one byte as two hexadecimal digits (using digits 0–9 and letters a–f), so you can write a SHA256 hash as a string of 64 numbers and letters—as I've done in the SHA256 hash of a file above.
- The hash is *chaotic*: that is, a small change in the input message will lead to a vastly different output hash. For example, the MD5 hash of the message “**mathNEWS** good!” is d2963ebe27c-3d10696a908754364de0c, while the MD5 hash of the message “**mathNEWS** food!” is 0205a4f9c1c1d16812a6af42937fd479. Notice how the input changed by a single letter, but the output changed completely.

These two facts combined lead to the reason why hashes are so common while downloading files. Most of us have been to the Davis Center library, so we know what bad internet connections are like. One of the things a bad internet connection can mean is that your file may stop downloading at 99%, and your browser may not realize it wasn't fully done and save it. Or some of the data may get corrupted on the way. Or (if you're important enough) KGB spies might sabotage your internet and send you a virus instead of the documents of national security you were downloading. Hashes can protect you from all of this.

When you download the file, you can compute the hash of the file you downloaded yourself. Then, you can compare the hash that was uploaded to the website, with the hash that you computed yourself. If the file they uploaded is the exact same as the file you downloaded, the hash will be the same! And you

will know that your download was successful. But if the file was even slightly malformed, corrupted, or otherwise changed, the hash will be completely different. And since the hash is fixed-size, it's only going to be a tiny extra bit of download even if the file you're checking is multiple gigabytes.

With all that said, not all hashes are created equal. Certain hashing algorithms (like SHA-1 and MD5) have been shown to be vulnerable to *collision attacks*. This probably won't affect you if you just want to check if your photo album downloaded right, but it can be a concern if you're expecting the hash algorithm to provide some sort of security to your data. A collision attack essentially lets someone take a particular hash value, and create a file with *any data of their own choosing* that has the same hash value. So if someone really wanted to mess with you, they could in theory swap out your download link with a malicious file, and when you go to check the hash of the file, it'll be the same as what the file creator gave you, so you'll think that you're safe from intrusion when you're really not!

This may seem like something that probably won't ever happen to you personally, and maybe it won't. But stuff you rely upon every day uses these hashing algorithms too. If you write software, git uses SHA-1 to track commits. Most online login systems store their users' passwords as hashes, so they can check them easily without having to store the actual passwords in their database. This is why companies often can't just email you your password when you forget it—they don't even have your password, they just have a hash of the password, and they check if the password you enter is correct by checking the hash. It's a fairly secure way (with some additional features like salting) to ensure that your passwords are safe, as long as hash functions aren't reversible.

Well, that's all for I have right now. Now you know what hashing algorithms are and why they're useful. Next issue, we'll take a look at how SHA-256, a real, secure hashing algorithm, is implemented. So stay tuned, and hope I'm not too lazy!

tendstofortytwo

References

Stevens, M., Bursztein, E., Karpman, P., Albertini, A., & Markov, Y. (2017, August). The first collision for full SHA-1. *Annual International Cryptology Conference* (pp. 570–596). Springer, Cham.

Anyone got a joint or
something to smoke?

PROF. TROY VASIGA

A POTENTIAL LEGAL CASE AGAINST ONE DIRECTION FROM LYRICS

CS 136 assignment 8 has been a special circle of hell.

To rectify my lack of understanding and time pushed towards watching really bad rom-coms, I wanted to sit down and listen to the NFL theme song and code for 6 hours. (You may judge me, but the NFL theme gets my ass in gear.) However, I came across music I downloaded when I was like ??? 8??? I don't know, time is a cube and isn't real. As I stared at Harry, Zayn, Louis, Liam, and Niall on the album cover, I made the mistake of pressing play.

Over the course of listening to the album, I heard some interesting lyrics. Since I've been researching ways to legally get out of my lease, missing Grade 12 Law class, and watching too many detective/cop shows, I decided to make a potential legal case against One Direction citing their lyrics from the Up All Night Deluxe Album.

So, welcome back to my NOT legal advice YouTube channel, let's get right into it.

“STAND UP”

Side note: I'm not going to lie, this song is a bop. I used to put it on repeat on my spherical pink speaker when I did my Canadian geography homework.

So put your hands up
Oh oh ohh oh
Cause it's a stand up

Anyways, this clearly sounds like demands from a classic bank robbery or like a Saint Valentine's Day Massacre-esque shoot out.

Side note: I USED TO THINK THIS LINE WAS SO SLICK. Where else would you get such an innovative use of a double entendre?

And I will steal us a car
And we will drive to the stars.
I will give you the moon.
It's the least I can do
If you give me the chance.

Stealing a car is classified under grand theft auto. Plus in order to launch anything into space from Earth, YOU NEED TO GET A PERMIT, as is stated in the Outer Space Treaty overseen by the UN. In addition, the Outer Space Treaty states “the Moon and other celestial bodies shall be used exclusively for peaceful purposes.” One could argue giving someone the moon is a capitalistic venture, enrage communist states, and inadvertently being a dispute which goes against exclusive use for peace.

Side note: Zayn's head on Gru's body from Despicable Me stealing the moon.

I'm a thief, I'm a thief
You can call me a thief
I'm a thief, I'm a thief

Obviously a clear declaration of guilt and theft. However, if they are lying and under oath, it would count as perjury.

Side note: What if creating a boyband was Simon Cowell's way of getting into countries and committing bank heists?

“ONE THING”

Now I'm climbing the walls
But you don't notice at all
This sounds like... breaking and entering.
Shot me out of the sky

If taken literally, shooting someone out of the sky is murder. If we interpret shot as shooting photos or taking a picture, it may infringe on privacy rights, right of publicity, and voyeurism. A prime example of legal action that could be taken is modelled in *Aubry v. Éditions Vice-Versa Inc.*

Fun lyric interpretation:

So get out, get out, get out of my head
And fall into my arms instead

I kind of just imagine how Zeus gave birth to Athena through his forehead, that might just be me though.

“UP ALL NIGHT”

The party's ending but it's now or never
Nobody's going home tonight

Now or never for what? However, given the theme of this piece, let's assume so law-breaking. Also if you're in/on private property and the owner doesn't want you there, it technically counts as trespassing. If this is a planned unlawful act, it is conspiracy.

Don't even care about the table breaking
We only wanna have a laugh

Obvious destruction of property and potentially reckless endangerment if someone got hurt. If one person commits the crime, then the rest of One Direction aids in covering up the situation, they are accessories after the fact.

Fun lyric interpretation:

I wanna stay up all night
And jump around until we see the sun

<https://www.youtube.com/watch?v=b0NHrFNZWh0>

“TAKEN”

I slept on your doorstep
 Begging for one chance

This really depends on whether or not the doorstep is public property (i.e. a sidewalk) and could potentially be trespassing.

You only love to see me breaking
 You only want me 'cause I'm taken
 You don't really want my heart

If these accusations are baseless and detrimental to my working relationships or character, this could be defamation of character.

“I WANT”

You could be preoccupied
 Different date, every night
 You just got to say the word
 But you're not into them at all
 You just want materials

Again with the defamation of character!

“SAVE YOU TONIGHT”

I, I wanna save you
 Wanna save your heart tonight
 He'll only break ya
 Leave you torn apart, oh

In law, if you believe someone is being endangered and do not act upon this belief, depending on the circumstances you may be committing reckless endangerment. If One Direction believes that my heart needs to be saved and my romantic partner will “break me” and “leave me torn apart,” they may be subject to reckless endangerment.

Oh now you're at home
 And he don't call
 Cause he don't adore ya
 To him you are just another doll

I mean, defamation of character right out of the gate. Also, how do they know that he's not calling? Stalking someone is illegal. So is cloning someone's phone. So is cyberstalking.

Side note: The definition of stalking is actually really loose, staring at someone and/or gift-giving could potentially be stalking.

Here's an informational pamphlet from Canada's Department of Justice:

https://www.justice.gc.ca/eng/rp-pr/cj-jp/fv-vf/stalk-harc/pdf/har_e-har_a.pdf

“GOTTA BE YOU”

Cause I'm the foolish one you anointed with your heart
 I tore it apart

Ok, this one is a doozy. So in the biblical definition of anoint, it means to ceremonially confer holy office upon someone. So in a way, we offered our heart to One Direction and they “tore it apart.” Theoretically, with the correct context, this could be like organ harvesting. Plus, if I am an organ donor and One Direction knows someone is in need of my heart for a heart transplant, it's premeditated murder and assassination.

And your actions speak louder than words

This is more of a PSA than a legal point, the absence of consent or “no” does not equate to consent. Legal verbal and/or written consent is of utmost importance!

—

That's all I have, for now, I hope you've laughed and/or learned some fun law things. I'd like to add, knowing the law and understanding your legal rights is an amazing thing. It helps you, your loved ones, and anyone who may need your help, defend themselves in the eyes of the law. Plus you may find important and/or eye-opening tidbits of information.

Thanks for tuning in, next time I'll be explaining why I think Esteban from Suite Life of Zack and Cody is an evil mastermind.

Eggo_Chuggo

PIAZZA**NOT A POEM**

Posting on the verge of a mental breakdown. “Cancel” culture. Can't write anything without sounding in-sane. Promoting cancel culture when it suits me. Bringing up *kinderwagen* on a STAT231 post. Denouncing cancel culture when it doesn't. The OP is about something completely unrelated. Fraught with anxiety. Remembering that everyone in the thread receives an email for every one of my dumb asinine comments. Thinking I'll get suspended. Not doing anything wrong. Professor replying passively and aggressively. Can't delete anonymous comments. I'm as politically correct as it gets anyway. Having been an “instructor-endorsed answerer” in 1A. Trying not to vomit. An ISA for CS135 was responding to me while browsing /trash/. If I become a Tesla shill, will I be unafraid of downvotes? Being nothing now. Missing MATH145. Not my grades, just djao. The soul leaving my body.

But **mathNEWS** is always there for me.

Anonymous Poet

RELATIONSHIPS ARE ALL ABOUT TEAMWORK: MICROSOFT TEAMS AS A DATING SITE

You may still be nursing the wound of not getting matched from the Aphrodite Project: Pandemic Edition... But no need to be sad any longer, 'cause your next place to find pandemic-era love has entered the stage!

It's new, it's shiny, it's IST-approved. Good-bye Skype; hello Teams! Microsoft Teams is the highly acclaimed communications platform that every University of Waterloo student has access to.

FEATURES!

Teams takes the cake in terms of features: no other platform looked at so far comes close. A real-time chat feature, complete with picture support, reactions, read-receipts, group chats, and reactions, allows you to chat smoothly and fluently with people—a tremendous improvement over the email-style DMs of competitors like Learn.

Audio calls and video calls are another feature Teams supports. Both systems are well-endowed with useful features like hand-raising, muting, screen-sharing, and even background-changing to simulate going to different places even during an online date!

A calendar with integrated scheduling features is built into Teams. You can send requests for a date easily and directly, and the recipient of the invitation can RSVP (or decline) right on the platform—the calendar is a sure fire way to make sure that everyone's schedules line up!

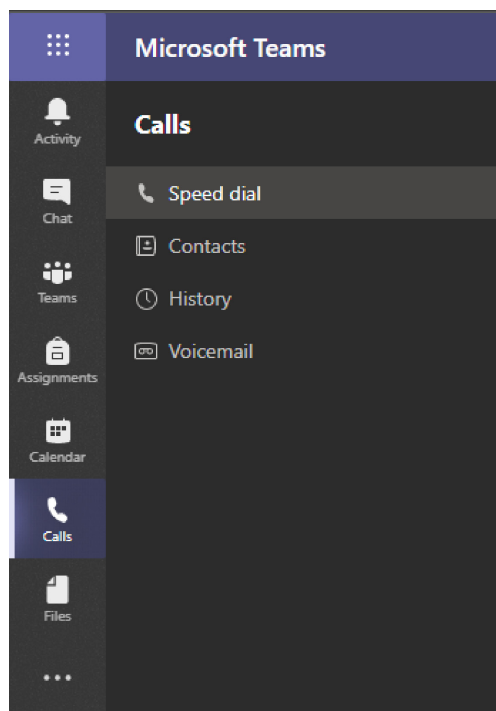


FIG 1. Microsoft Teams' sidebar, showing off a strong assortment of features.

All sorts of neat dates are made possible through Teams' features. From coordinating to executing, the teamwork of setting up dates is made easy by Teams!

MATCHMAKING?

Where Teams falls behind is in discoverability. While other dating sites like Learn or Piazza match you up based on common interests such as classes, Teams has, well, Teams. These groups are created by Faculty members for specific purposes, and unless there's a special organization that you're part of, it may be difficult to meet people.

When it comes to dating sites, the ability to meet compatible people is critical to success. Sadly, Teams has let this side of dating platforms fall by the wayside. There aren't any groups of people you're added to by default to discover potential partners; neither are there public virtual spaces to connect.

The profile feature is limited to a small thumbnail photo and a Twitter-style 280-word bio, which is a different style from the long-form profiles that other sites like Learn/Piazza provide. Perhaps this is a new format designed with the web-surfing, fast and flighty modern generation in mind?

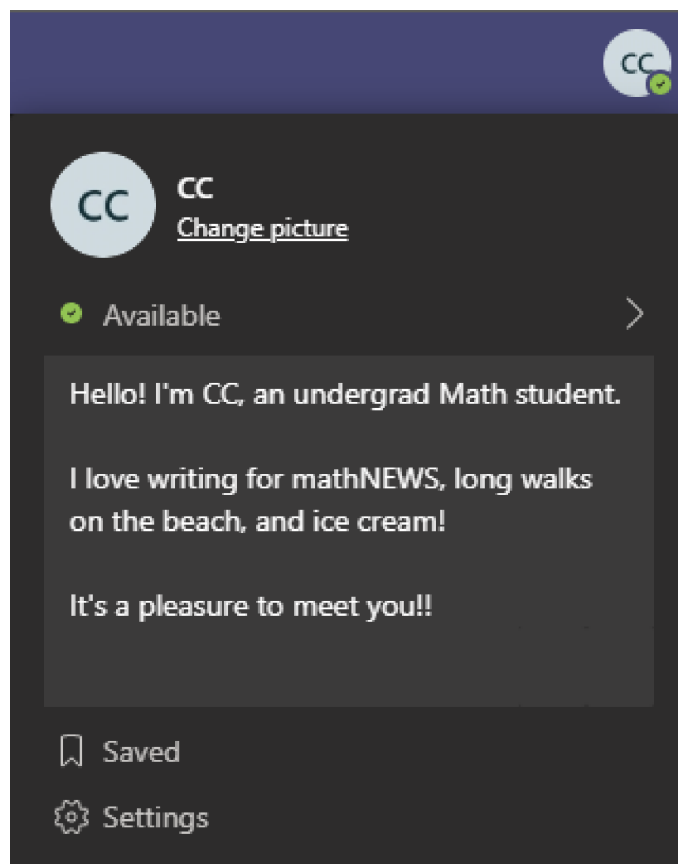


FIG 2. Weak profile and matchmaking systems beg the question: why did Microsoft put so much effort into fancy features, then neglect such a vital aspect?

Every UWaterloo student has a Teams account, and in an attempt at redemption, Microsoft allows one to search anyone up and DM them through the search function of Teams.

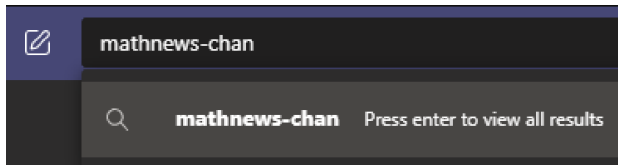


FIG 3. Searching someone up on Teams is easy and quick.

Perhaps Microsoft has some special psychology research that suggests such an approach will result in higher-quality matches being made organically as people reach out through by themselves, instead of being presented with options? Only time, and experience, will tell.

SUPPORT & PRICING

Teams comes as a mobile, web, or desktop app, allowing you to keep up to *date* on all your romantic forays no matter where you are! In addition, IST even offers a training course on how to use Teams to make sure that you know what you're doing.¹

Integrated with Microsoft Office, Teams supports file sharing and other useful organizational features with various UWaterloo Microsoft Office apps.

University of Waterloo students have free access to Teams.

IN CONCLUSION

Without a doubt, Microsoft Teams is one of the strongest contenders for online dating sites. It sweeps away the competition in terms of features and can singlehandedly facilitate a variety of types of dates, but falls short when it comes to actually matching people together.

At the end of the day, Microsoft has put together a polished, feature-rich, and well-integrated platform. The choice of name is apt: when you start a relationship, you start a Team!

CC

1. <https://uwaterloo.ca/microsoft-teams/>

PROGRESS?

I am standing on a cloud thats getting smaller or I'm growing. I can see the whole world just not my own. People aren't ants they are microbes. All I see is the aftermath. I watch as the forest recedes into itself. I watch as the oceans reclaim the shores. I watch as the smog envelops, and darkens. How do you cure a disease you can't see? How do you try a crime that hasn't been committed yet?

ITSH

A SONNET ABOUT HASH TABLES

Direct addressing is a good way
To implement a dictionary where
Positive integers are the keys k ,
But if M is not known, do not despair,
Discover now the magic of hashing!
Use a hash function and a hash table,
Mapping keys, then directly addressing,
It's the stuff of data structure fables.
But be wary of deadly collisions,
As the hash function is not injective,
Whatever you do is your decision,
Cuckoo hashing? Sure, your prerogative.
Learn so much more in CS 240,
Then write poems so terribly corny.

Finchey

EPISODE 6: MATH 239 GRAPH COLOURING

On the following page, enjoy episode six of MathSoc's educational cartoons series: [MATH 239 Graph Colouring!](#) This cartoon attempts to connect graph colouring to maps and clear up several misconceptions. If you have any feedback please email Gavin Orok at gjorok@uwaterloo.ca or fill out the following survey: https://bit.ly/cartoon_feedback. For each unique educational cartoon we produce that you give feedback on through this survey, your name will be entered in a draw. At the end of the term one person from this draw will be chosen to win a \$25 gift card prize!

Gavin Orok

You should ~~write~~ be an editor for mathNEWS.

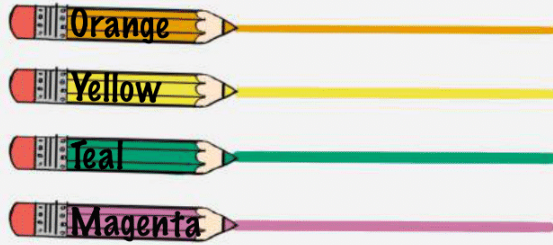
(I swear it's not as bad as I make it sound.)

A mathNEWS EDITOR WHO WANTS
TO GET THE HELL OUT OF THIS
MADHOUSE AND RUN DEFINITELY
SECURE THE FUTURE OF THE PAPER

Math 239: Graph Colouring

Idea by: Gavin Orok | Story by: MathSoc | Art by: Alvina Cheng (@etanearth)

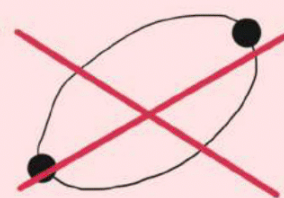
Let's "illustrate" graph colouring using maps!



Assume you are working with SIMPLE GRAPHS:

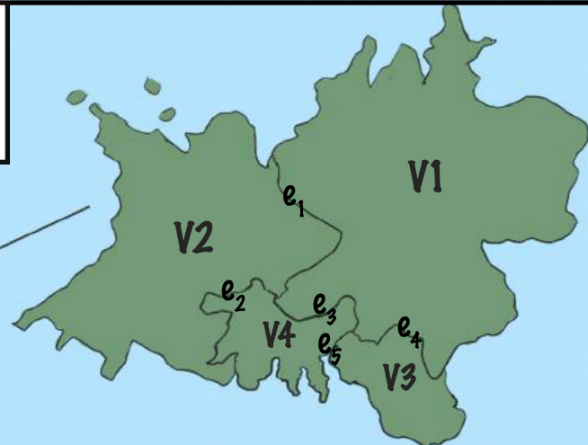
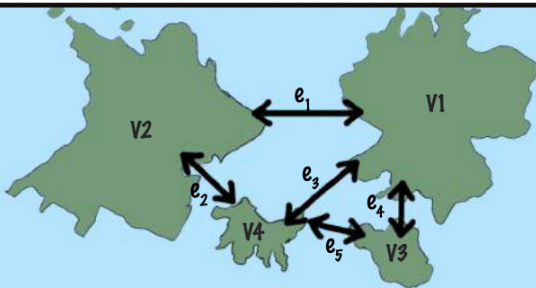


No loops to the same vertex

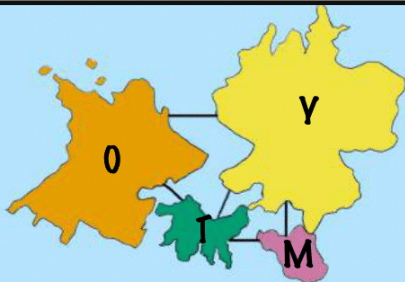


At most one edge per vertex pair

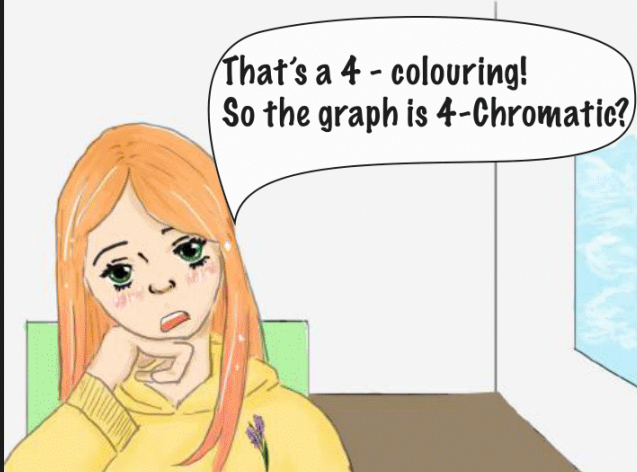
Think of a graph as a map where vertices are countries and edges are borders between adjacent countries.



In a K -colouring of a graph, we assign K colours to the vertices so adjacent vertices are different colours.



So we use K pencil crayons to colour in a map and distinguish neighbouring countries.

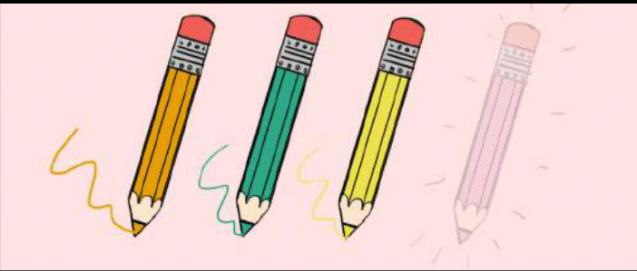


The graph is 4-COLOURABLE NOT 4-Chromatic.

Math 239: Graph Colouring

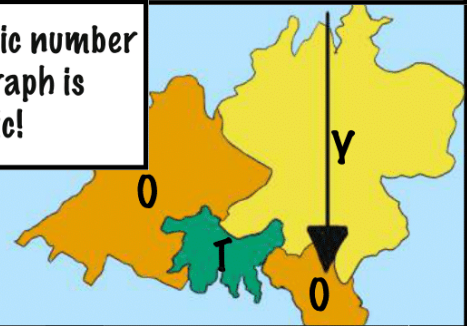
Idea by: Gavin Orok | Story by: MathSoc | Art by: Alvina Cheng (@etaneart)

The chromatic number is where you are as stingy as possible with different pencil crayons.



The magenta and orange countries don't share a border. Magenta isn't needed!

The chromatic number is 3, so the graph is 3 - chromatic!



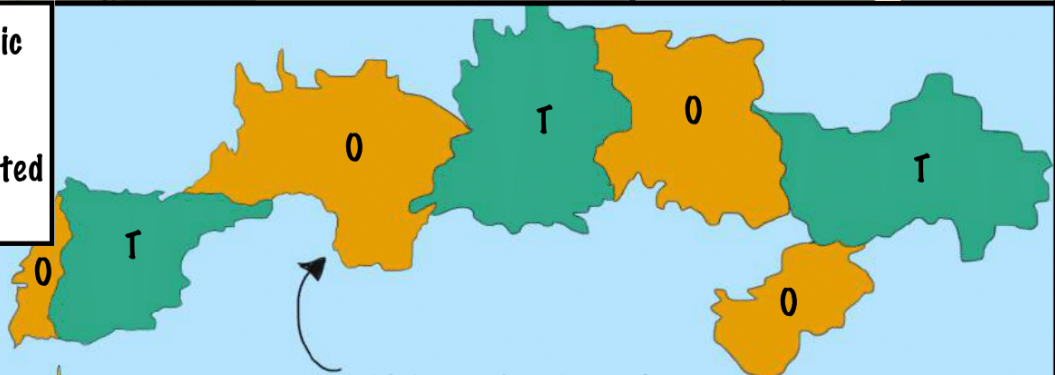
So graphs with more vertices and edges have higher chromatic numbers?



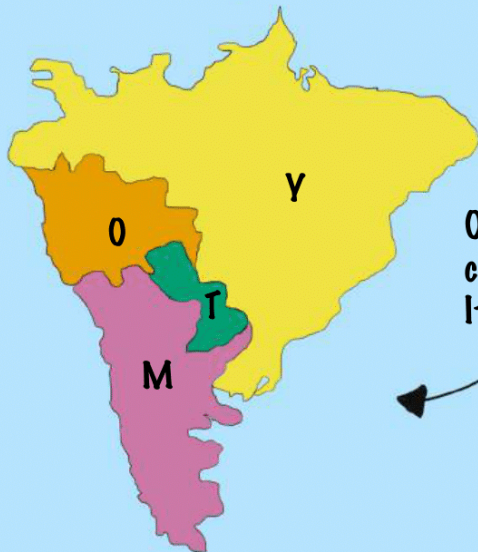
Not necessarily!



Look at chromatic numbers as a measure of how mutually connected vertices are.



THIS map has lots of countries and borders but few countries share neighbours. It is 2-CHROMATIC.



On the other hand, THIS map only has four countries but they are all adjacent. It is 4-CHROMATIC.

More mutual connections means there must be more colours!

THE WEBMD ARTICLE THAT DOESN'T EXIST (FOR GOOD REASON)

Imposter Syndrome (IS) is a serious illness that affects millions of Americans every year. And if it affects America, then it probably affects Canada. Admittedly, we don't really know. Canada is too far north for us to conduct statistical research. Those affected by the disease feel like they do not belong or have deceived others around them to believe they are more competent than they know themselves to be. Discussed in the latest module of "Waterloo Ready", there is still controversy regarding this illness, as some have artfully characterized it as "being a lil' bitch" (*my supportive anonymous friend*, 2020).

TYPES

IS comes in many forms, but most cases fall into at least one of the following general categories:

The math student: this individual suffers from absurd perfectionism, obsessing over the rigor of their proof for so long that they don't notice forgetting a negative sign on page 4. Fortunately, these slight miscalculations and arithmetic errors aren't usually indicative of failure, as math students rarely find themselves actually working with numbers. Look to Andrew Wiles for inspiration.

The med student: this person is often seeking to live the Grey's Anatomy life in reality. This leads to unnecessary effort and distaste for free time, because they believe working any less than 21 hours a day will never amount to any measure of success. Passions and hobbies are abandoned for the sake of a career and professional validation. Look to Dr. House for a true role model.

The physics student: this individual holds the great geniuses of our era close to their heart — Albert Einstein, Sir Isaac Newton, Niels Bohr. But this may unintentionally become an unrealistic standard of having to be a "natural genius." The physics student may then assume a suave, chill personality to impress the chemistry students in their PHYS121 class, frequently complaining about how general relativity should be taught instead of Newtonian physics because conceptual precision should never be sacrificed; but will subsequently come home depressed with the knowledge that they watch MinutePhysics YouTube videos instead of their online lectures. Look to Wilhelm Roentgen for an example of when all it takes for a major breakthrough is a small accident, not ultimate intellectual superiority.

The arts student: this student is pursuing the soloist persona. Armed with stories of mad artists locking themselves into a room for years and creating awe-inspiring pieces, for true art should be an individual creation, portraying the soul of the artist alone. Salvador Dalí and Vincent Van Gogh are the true inspirations for this construct, for they made their art practically isolated from society. Asking for help is unthinkable for an individual suffering from this type of IS,

for that may lead to people assuming the absolute worst — that they do not belong. Look to musicians to see that collaboration and art often, somewhat unfortunately, appear together.

The engineer: This human(?) being assumes they must be an expert before learning anything. Through the fear that they do not know enough, they present themselves as knowing too much. Just as the other types of IS, this is often caused by low self-esteem. However, no research yet exists on how to raise an engineer student's self esteem, for their general sense of self is already three orders of magnitude more inflated than average.

DIAGNOSIS

Your doctor may do a physical exam and blood tests to make sure something else isn't causing your symptoms. They will also talk with you about your feelings, thoughts, and habits. Unfortunately, your doctor may also be inexplicably suffering from IS, so be aware that 96% of his concentration may be on fooling the receptionist that a med degree from some hershey highway like the University of Manitoba warrants placing actual human lives in his very sweaty hands.

CAUSES

While it is uncertain whether there is a genetic factor at play in this illness, the data clearly illustrates that IS is directly linked to being a Waterloo student. Additionally, more severe instances of IS have been found to be disproportionately more common when an individual is or has a history of being a **mathNEWS** writer. Health authorities are warning against such mentally dangerous activities, as participating may place you at a much greater risk than normal.

TREATMENTS

There is no current available cure for long term IS. However, as with many chronic illnesses, there are methods and treatments that help those afflicted. Recognizing and rewarding yourself for your genuine accomplishments, reaching out to family and friends for support, remembering the skills that you have already developed over your academic or professional career, and any other verbs that start with the letter R will help you manage and live with IS.

In another approach, you could also just drop everything and become a zucchini farmer on the prairies. This can be considered as a preventative treatment, allowing you to live in a blissful existence isolated far from anyone that could be potentially better than you. It is also hypothesized that having absolutely no goals may completely eradicate IS. Scientists are awaiting the oncoming online fall term to assess this hypothesis using frosh data.

N REASONS TO PURSUE A PLAN COMBINATION

- It increases the characters/cm² of your diploma.
- Think of each combination you get as a level-up. A single major is Level 1. Go for three majors with options, and you can get to Level 5 and beyond.
- If one set of advisors screws you over, you can always go to the advisors for your other plans.
- You get to sound all posh and snobby when telling people of your degree. "Excuse me, but I don't have a Bachelor of Computer Science. I have a *Bachelor of Mathematics in Computer Science and Applied Mathematics, minors in Biochemistry and Political Science, specializations in Artificial Intelligence and Engineering: Heat and Mass Transfer*. Please get it correctly the next time."
- It's fun to learn more stuff. Especially when no one else is learning it.
- You get clout within your friends. "Nah, I only have a joint Statistics and Computational Math; I'm not insane enough to go for a double major. But *that guy*...he's insane."
- Watch interviewers' heads explode as they struggle to process how one person could have so many academic interests. Works especially well on engineers.
- Look, you're in math, you were going to be antisocial regardless how many courses you took per term. Pursuing a plan combination isn't going to make a difference.

quantum goose

IN THIS SONNET, I JUST COMPLAIN ABOUT STAT 231

STAT 231: Statistics, they call it,
 Its reputation I had not believed,
 But now, dear reader, to you I admit,
 'Tis all true: it is the worst course conceived,
 Not Struthers, Adcock, nor e'en Banerjee
 Bestow insight and elucidation,
 The slides and the course notes are so crappy,
 What e'en is the Chi-squared Distribution?
 I will tell you a bird course this is not,
 Unless you like feeling completely lost,
 The assignments and quizzes suck a lot,
 I'd drop the course if it weren't for the cost.
 I'm mostly exaggerating. Mostly.
 Still can't wait 'til it's over finally.

Finchey

N REASONS YOU SHOULD GO BALD TODAY

- It's easy and breezy
- It increases friction so when you put on a shirt it feels like a head massage
- It's a gender-neutral hairstyle
- You can use the pandemic as a reason to go bald
- Your head gains a sandpaper-like texture, which is ideal for home improvement projects
- Cures disease (like head lice)
- It's free
- More aerodynamic
- It makes your hearing better
- It lets you discover all of your secret moles
- You can prove that you don't have any brain implants
- So you can hear your mom scream when she sees that you're bald
- You can use less shampoo (you still need some for your scalp though)

Hair Expert

N IDEAS PINK CAPTAINS CAN DO TO INCREASE FIRST YEAR ENGAGEMENT

Waterloo Math Ready is the innovative and exciting new online program to welcome incoming Math First Years to Waterloo! Teams (the platform it's running on) has been a little quiet, so without further ado: strategies Pink Captains (the upper-years running events) can use to get First Years participating!

- Mark everything you write as an announcement, important, and tag the whole channel so First Years get emailed every time you say something
- Offer a live tour of campus
- Offer free bubble tea to the first M people to introduce themselves
- "Don't use Microsoft Teams." — A first year student interviewed by **mathNEWS**
- Pray to Mr. Goose for more participation
- Develop a COVID-19 vaccine and distribute it to everyone so the university can re-open and you can meet in person instead of online

CC

P.S. If you're a First Year Math student, come join Waterloo Math Ready—we don't bite!

elseWHEN: A LOOK INTO THE PAST, FROM THE PAST...

Ah, **elseWHEN**, the recurring segment that takes us back to the olden days of yonder, when **mathNEWS** was still on a pacifier—figuratively speaking—and the world was in greyscale. This issue, I present to you The Unnatural Historian's Unnatural History, published in V110i6 on Friday July 24, 2009, eleven years ago to the day. The article recounts the mythical nascency and ascent of **mathNEWS** with whimsy and delightful delivery. It's the definitive version of the legend, at least in my humble opinion. Without further ado, here it is in all its glory:

In the beginning...
there was *math*.
Then we tacked **NEWS** onto it.
But that's not the whole story.
For the whole story we must go back.
Waaaaaaay back.
To the start of the epoch.
Ok, shortly after the epoch.
Give it a year.
The mathies were restless.
They had been doing their math for a full graduating class.
But they didn't feel satisfied.
There must have been more.
Something beyond the integrals,
the analysis,
and the batch jobs that suffused their existence.
Great ground was being broken in math and CS!
But the mathies no longer wished to use their creativity!
So one day,

In 1973.
They wrote an article.
And it began like this...
"They did and it didn't"
And then they wrote about real news,
they reported about the nice things.
Like the C & D.
When it was just a stand on the 3rd floor.
And for a time... it was good.
And then it got better!
Puzzles were placed.
gridWORDS were generated.
profQUOTES were professed.
And columns came and went as students graduated.
And that's the truth.
Or so I shall tell you.
The real story is way more exciting.
It has dinosaurs.
And high powered lasers.
And several rings of power.
I recall a time machine was involved.
How did you think the science paper *Dark Matter* came about?
At one point there was a division by zero.
The less said about that, the better.
In either case,
the mathies rejoiced.
For they had **mathNEWS!**

clarified

N WAYS TO MAKE SENSE OF NOT GETTING A MATCH FROM THE APHRODITE PROJECT: PANDEMIC EDITION

- Your perfect match missed the deadline for signing up.
- Your perfect match was 2 inches taller than you; this was a dealbreaker.
- Your perfect match was 2 inches shorter than you; this was a dealbreaker.
- Your perfect match filled out the questionnaire while under the influence so their answers are not entirely accurate.
- Your perfect match had their questionnaire filled out for them by a friend who didn't know them like they should.
- Your perfect match filled out their questionnaire while listening to an emotionally charged album, and the music affected their responses.
- Your perfect match doesn't go to UWaterloo.
- Your perfect match doesn't go to UWaterloo, yet.
- Your perfect match doesn't go to university.
- Your perfect match is seeing someone that is not their perfect match.
- Your perfect match is struggling to get over someone that is not their perfect match.
- Your perfect match is not ready for a relationship at the moment.
- You are not yet ready for a relationship at the moment.

Deriving for Dick

I love grad students.
They'll do anything you
tell them to.

PROF. ROSS WILLARD

N WAYS TO GET THIS ENTIRE ISSUE BANNED IN MAINLAND CHINA

I feel like it is important to add this disclaimer:

Just because President Trump, the Trump administration, and the American government are corrupt and responsible for some human rights atrocities (such as detaining and separating families at the US-Mexican border, teargassing a crowd of peaceful protesters, police brutality, etc.) does NOT mean that the American PEOPLE are responsible for it. Nor does it mean that American people are bad and should be hated for the actions of their government.

Similarly, it is important to emphasize that the purpose of this article is NOT to spread xenophobia to Chinese PEOPLE. I am ethnically Chinese. But the **Chinese Communist Party** (CCP) is very corrupt and has committed many human rights atrocities that I wish to raise awareness of. Thanks to the free speech guaranteed in Canada, I'm able to write this article. This article does NOT condone any hate against Chinese people and the writer is appalled that such people exist.

Without further ado, here's the listicle:

- 1989 Tiananmen Square Massacre
- Respect Hong Kong's Autonomy!!!
- Free Michael Kovrig and Michael Spavor from arbitrary detention
- 1984 Orwellian Police State
- Taiwan is an independent country!
- Free Tibet!
- The Great Proletarian Cultural Revolution
- The Great Leap Forward
- Winnie the Pooh
- Stop Organ Harvesting
- Amnesty for Falun Gong
- Amnesty for Uyghurs
- Stop Christian Prosecution
- End the 'Re-education' camps!
- Freedom of Religion
- Freedom of Speech
- The Chinese Communist Party covered up the 'CCP virus' (Covid-19)
- So, don't let Li Wenliang die in vain
- W.H.O. corruption and bribery
- CCP Mask Hoarding
- The Anti-Rightist Struggle
- Human Rights
- Democratization
- Freedom
- Transparency
- Multi-party system
- Free elections
- Right to a reasonable trial in front of a jury
- Transparency for Capital Punishment sentences
- Liu Xiaobo
- The South China Sea and The Nine-Dash Line doesn't belong to the CCP

- Don't trust the CCP with international agreements
- Stop the 'Whataboutism' diplomacy
- Historical Revisionism
- End Neo-Imperialism in Africa
- Redact Hong Kong's 'National' 'Security' 'Law'
- Cooperation works both ways, don't expect other countries to help you if you won't hold up your end of your deal with no extra strings attached.

Source: Thanks to the lack of internet censorship in Canada, one can Google all these terms and get more details about them from the internet. But there is a source that has helped me quite a bit:

Shoutout to the YouTube channel "*China Uncensored*" for inspiring me to make this article and for helping me research. They are a satire news channel that covers questionable government events in both China and the USA (on their second channel "*America Uncovered*"). If you're looking for a humorous place to get your news from, I recommend checking out at least one of their channels.

CCP Virus Spreads News

THE PURE MATH, APPLIED MATH, AND COMBINATORICS & OPTIMIZATION CLUB'S PROBLEM OF THE ISSUE

Hello friends,

Here is a nice light exercise to while away the quarantine hours—and possibly win you a prize.

Let k and n be positive integers. Derive, with proof, a formula for the number of non-trivial arithmetic progressions* of length k whose members are all positive integers at most n .

*We shall define a non-trivial arithmetic progression of length k whose members are all positive integers at most n to be a k -element subset $S \subseteq \{1, 2, \dots, n\}$ such that if $S = \{a_1, a_2, \dots, a_k\}$ with $a_1 < a_2 < \dots < a_k$, then $a_2 - a_1 = a_3 - a_2 = \dots = a_k - a_{k-1}$.

Submit your solution to pmclub@gmail.com.

INCOMING DEAN OF MATH SURPRISED TO FIND PRINT COPY OF THIS ISSUE ON HIS DESK

WATERLOO—Mark Giesbrecht, incoming Dean of Mathematics, entered his office on Monday morning expecting a fresh, clean working space—only to be greeted with a single copy of **mathNEWS** v143i5 on his desk.

“How did this rag get here?!” the enraged Dr. Giesbrecht shouted to his empty office as he waved the rogue issue around in his hand. “Kevin told me he locked the door! MC wasn't open until today! **mathNEWS** isn't even printing copies this term!”

The Dean became even more infuriated when he opened the issue to this article.

“Wha...what is this nonsense!” Dr. Giesbrecht screeched, his face turning redder than a sea of red wine. “How did they predict all of this? The author isn't even an editor!”

Witnesses say that for the rest of the workday, Dr. Giesbrecht would do nothing but pace around the office while muttering under his breath and randomly checking various nooks and crevices, only leaving to check the bathroom every five minutes. That this was witnessed is strange, as no one else but Dr. Giesbrecht was in the Dean's office for the entire day.

As of press time, Dr. Giesbrecht had not discovered the seventeen other copies of this issue hidden around his office, his car, his house, and his jacket.

quantum goose

N BOOKS I LOADED ONTO MY KINDLE IN HOPES OF GETTING BACK INTO THE HABIT OF READING

- *Superintelligence* by Nick Bostrom
- *Brave New World* by Aldous Huxley
- The entire *Harry Potter* series by JK Rowling
- *Pride and Prejudice* by Jane Austen
- *Think* by Simon Blackburn
- *Kindle Paperwhite User's Guide, 17th Ed.* by Amazon

tendstofortytwo

I WANTED TO WRITE AN ARTICLE

I want to write an article, but it's really hard since I'm never a witty person that can think of ideas on the spot. I was never a creative person, so this article is going to be boring. See, I'm already rambling about literally nothing. Which is a good skill to have in life, because you can bullshit pretty much anything. Using words similar to “nevertheless,” “however,” etc., makes your speech sound 10x more professional and well-thought.

However, you must acknowledge the fact that this method heavily on the subject and primary target of the audience. You may also have noticed that the sentence above is totally fluffed out and is literally of no use to you in pursuing anything significant in your life.

Fun fact of the day, if you put all your blood vessels in your body in a straight line, you would actually die.

TurboMoist

STUDENT CAN'T WAIT UNTIL SCHOOL OVER SO HE CAN MISS SCHOOL AGAIN



UW Unprint

Hmm, well let's pretend this is right.

PROF. IAN MUNRO

LOCAL WATERLOO MATH STUDENT EXTREMELY PISSED THAT HE SOLVED 99% OF THE MATHSOC PUZZLE CHALLENGE

This student, who wishes to remain anonymous, says that as soon as he glanced at the problem, he recognized the NATO phonetic alphabet at once. He further claims, that after seeing "Lima Alpha X-Ray," the *very first thing* that came to his mind was the Los Angeles airport, thanks to a certain song on the *Need For Speed: Underground 2* soundtrack. The student then goes as far as to insinuate that he even found a location plotter online, and plotted these locations on a map, and connected them with lines! But that isn't even the worst of it. The boldest, most outlandish claim of this student is that he *could clearly see two of the four alphabets (C and E) that formed the answer, and that's when he gave up!* Now, we aren't ones to just take someone's word for it when they say they totally almost but not quite did something, but you have to admit that this student, had all this actually transpired, would have felt so deep and utter remorse on seeing the solution, felt so lonely and sad on having given up mere inches away from his moment of triumph. It would truly be a sad thing to witness this.

At least † he got the second puzzle right.

tendstofortytwo

N SOLID PIECES OF ADVICE FROM THE ASTROLOGY APP I DOWNLOADED FOR LAUGHS

- "Don't take yourself too seriously today."
- "Watch a cooking video. Then do it yourself."
- "You're not your best self when you evade. Fail. Get up. Then fail again. Do this over and over, until you've trained yourself to take your lessons standing up."
- "A lack of anxiety makes you more interesting to be around." (I...I'm in this photo and I don't like it.)
- "You control what you say but not what other people hear."
- "You're so skilled at reflecting just what everyone wants to see. You won't learn what you need and desire until you put down the mirror and start listening to yourself."
- "Your need to be perfect reveals a primary uncertainty. It is far healthier to be flawed than insecure."
- "You might feel obligated to punish other people for dissatisfaction. Don't. Instead, try to seek out variety. First one foot, then the other."

This app is called Co-star, if you want to join me in receiving some unsolicited tough love from astrology...

royal no.69 milk tea

ISSN 0705-0410

UW'S BASTION OF ERUDITE THOUGHT SINCE 1973

mathNEWS is a normally fortnightly publication, funded by and responsible to the undergraduate math students of the University of Waterloo, as represented by the Mathematics Society of the University of Waterloo, hereafter referred to as MathSoc. mathNEWS is editorially independent of MathSoc. Content is the responsibility of the mathNEWS editors; however, any opinions expressed herein are those of the authors and not necessarily those of MathSoc or mathNEWS. Current and back issues of mathNEWS are available electronically via the World Wide Web at <http://mathnews.uwaterloo.ca/>. Send your correspondence to: mathNEWS, MC3030, University of Waterloo, 200 University Ave. W., Waterloo, Ontario, Canada, N2L 3G1, or to userid.mathnews@gmail.com on the Internet.

This work is licensed under the Creative Commons Attribution-Noncommercial-No Derivative Works 2.5 Canada License. To view a copy of this license, visit <https://creativecommons.org/licenses/by-nc-nd/2.5/ca/> or send a letter to Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA. Terms may be renegotiated by contacting the mathNEWS Editorial Team.



lookAHEAD

SUN JULY 26

MON JULY 27

TUE JULY 28

WED JULY 29

THU JULY 30

FRI JULY 31

SAT AUG 1

mathNEWS 143.6 prod—oh wait, that's next week...

View next term's schedule and appointments

National Avocado Day

SUN AUG 2

MON AUG 3

TUE AUG 4

WED AUG 5

THU AUG 6

FRI AUG 7

SAT AUG 8

Civic Day
mathNEWS 143.6
production night

Drop/Add period begins for returning students

Drop/Add period begins for returning students
Last day of (online) classes

Final assessment period begins
mathNEWS 143.6 published

National Sneak Some Zucchini Into your Neighbour's Porch Day

LAST WEEK'S gridSOLUTION

A	L	W	A	Y	S		K	E	R	N	E	L					
C			P			Q	U		I			O					
C			O		Y	U	R		Y			U					
R	E	F	L	E	X	A	N	I	A	C	I	N					
U			L			D			D			G					
E	C	H	O			L	I	R	A	S	H	Y	D	E			
						A	I	N			I						
						C	O	N	S	T	E	L	A	T	I	O	N
						T			H	L	L	K			G		
S	I	R	E			E	X	I	L	E		C	R	O	P		
T						L	O		E						A		
A	T	O	M	I	C				C	A	Y	L	E		Y		
R						I	O			H					D		
C						R				H	U				A		
H	O	M	A	G	E					M	O	N	D	A	Y		

"HEY WISE GUY, WHERE'S THIS WEEK'S gridWORD?"

You, my friend, have dedicated so much of your heart to **mathNEWS** that not only are you taking the time to read the **lookAHEAD** of an online-only issue, you have also keenly noticed the lack of a **gridWORD** gracing its penultimate page. And for that, I thank you. I think this paper is so blessed to have such dedicated and invested readers. People like you give me hope.

The truth is that while I was doing layout, there was no way I could reserve a page for the **gridWORD** without cutting out some articles or janking up the spacing between everything. So it had to go. Sad day, I know. On the bright side, I was able to fill in this gap in the **lookAHEAD** by babbling on about the **gridWORD**. See, there's a silver lining to every cloud!

clarified

otherNEWS is made technically possible by club executives of the Math Faculty.

I say "technically" because if they had sent us more news this week, this box wouldn't be here.

THE **mathNEWS** EDITOR WHO PUTS THE "NEWS" IN **mathNEWS**