



## "WHAT SHOULD WE DO WITH ALL THE BACK ISSUES\*?"

\*BACK ISSUES BEING THE OLD, ALREADY-PRINTED ISSUES OF mathNEWS LYING AROUND THE OFFICE.

Here we are. Another issue of mathNEWS.

I have class in fifteen minutes and I am in a large amount of pain. Please, why has god forsaken me?

itorED  
Editor, mathNEWS

**GOD DOESN'T EXIST. COUNTEREXAMPLE: RIGHT NOW. QEDMF.**

stapLED  
Editor, mathNEWS

...I'm not quite sure what happened there, but for the sake of my other editors' sanity I should probably take over.

Welcome to yet another glorious term of mathNEWS! And also welcome to Spring term, I guess, but who really cares about that. Let's be real, anyone who is actually reading this practically lives and breathes mathNEWS (and we love you for it <3).

So yeah. The back issues. Us editors were cleaning up the mathNEWS office for probably the first time in a decade and found several boxes of issues from prior terms. We don't really know what to do with them. If you're missing mathNEWS issues from your framed collection, then swing by the office to pick some up before we burn them or some shit before we go with one of the actually reasonable suggestions.

Anyways, in this not-at-all-a-back-issue that you're reading right now, we've got the first appearance of two new mathNEWS editors, stapLED and yclepED! They're both really cool and you should definitely give them high fives when you pass them in the hall. It's also, sadly, the last appearance of a much beloved gridMASTER, Zethar. He will be sorely missed. The number of aneurysms character-building challenges he gave us will not, however. Not to fear, a successor has been knighted! Zethar assures us he will be up to the challenge.

That's all for now. Here's to a good term!

swindLED  
Editor, mathNEWS

NEW&CONFUSED | Fold a giant Mr. Goose.

NITRIC ACID | Giant bonfire on VI Green.

AC | The honking lord demands sacrifice (nesting material).

WALDO@<3.LE-GASP.CA | Donate them to libraries and schools across Canada.

SOVIET CANADIAN | Build a little fort.

SIGSEGV | Hold a book burning.

DIMINUTIVE REX | Eat them. Eat them all. Don't stop stuffing paper in your mouth, Unhinge your jaw and insert back issues upon back issues until the paper fills up the unending void within yourself.

TRISTAN POTTER | Gather "collections" of mathNEWS for specific terms or events (Pi Day) to then sell to alumni.

VARIOUS PSEUDONYMS | Cover every square inch of MC with back issues.

YCLYPED | Give every person at UW a single sheet of a back issue to make a paper airplane, then someone counts to three and we all launch them in the direction of Laurier at the exact same time.

STAPLED | Make some nice, math-themed piñatas. Paper mâché, anyone?

TBDED | Form a paper mâché teepee to act as an extension of the mathNEWS office.

SWINDLED | Load them into a cargo plane and drop them over the UofT campus, like they used to do with propaganda pamphlets.

ITORED | Baptize all new mathNEWS readers, writers and editors alike in a deep river of old issues.

## ARTICLE OF THE ISSUE

The article of the issue for mathNEWS 137.1 goes to New&Confused for What is an Actuary?. Getting actually informative articles is rare enough these days, and being the only article actually about math doesn't hurt either.

You can come by the mathNEWS office to pick up your prize of a \$25 gift card to Conestoga mall, whenever an editor is in the office. I should warn you though, we have a tendency to sink into the floor when we sense people who want to talk to us, so you'd best come by when we least expect it.

swindLED  
Editor, mathNEWS

mathNEWS is awesome. Proof: this issue. QEDMF.

ANUJ OPAL, mathNEWS EDITOR FOR SPRING 2018  
ALONG WITH ESTHER AHN, CLYDE BROWN, HEATHER STONEHOUSE AND MICHELLE ZHU

# mathASKS 137.1

FEATURING PROF. ALFRED MENEZES

## NOT A 5 YEAR OLD: HOW WOULD YOU EXPLAIN ELLIPTIC CURVE CRYPTOGRAPHY TO A 5 YEAR OLD?

Here is an explanation that should be accessible to five-year-olds, provided they have taken MATH 135.

An elliptic curve is a special kind ("genus one") of algebraic curve. One considers the set of points on such a curve whose coordinates are integers modulo a prime  $p$ , and then endows this finite set with a certain (mathematically natural) addition operation. It turns out that the problem of deciding how many times a point  $P$  on the curve was added to itself to obtain a second point  $Q$  on the curve is computationally challenging, and in particular is significantly harder than the problem of integer factorization. The former problem is the basis for the security of elliptic curve key agreement and signature schemes that are rapidly replacing RSA in internet applications.

## FRACTAL: IF NOT CRYPTOGRAPHY, WHAT CAREER WOULD YOU HAVE PURSUED INSTEAD?

At the beginning of my Master's at UW, I was torn between studying cryptography and algebraic combinatorics. If I had chosen algebraic combinatorics and was successful in research, then I might have been lucky enough to secure a research or teaching position at a university. However, the academic job market was quite dismal when I completed my PhD in the early 1990s, and so I likely would have ended up as a software developer (my undergrad degree at UW was in computer science and combinatorics & optimization).

## BORED: WHICH AUTHOR OR PIECE OF LITERATURE WOULD YOU RECOMMEND ABOVE ALL OTHERS?

I read very little these days, a sad consequence of my obsession with work and of time wasted on the internet (mostly reading news, not reddit). The most recent book that I enjoyed was Cathy O'Neil's "Weapons of Math Destruction", an eye-opening account of the destructive power of mathematics (especially machine learning and data science) in advertising, education, banking and finance.

## JOHN DOE: DO YOU HAVE ADVICE FOR STUDENTS WISHING TO TAKE CO 485?

CO 485 (The Mathematics of Public-Key Cryptography) is a reasonably self-contained course. Its only prerequisite, which the instructor is usually willing to waive, is a course in abstract algebra. The course has more depth than CO 487 (Applied Cryptography), but not the breadth. Students are exposed to a lot of pretty ideas that lie in the intersection of algorithms, complexity theory, number theory, and cryptography.

Noted reddit celebrity, u/djao, will be teaching CO 485 in Fall 2018. If you take the course, make sure you request that he covers his awesome quantum-safe isogeny-based key agreement scheme.

## HELLO KITTY: DO YOU HAVE A FAVOURITE TYPE OF CAT?

I have never been a pet owner. However, based on the inordinate amount of time I spend watching cat videos on the internet, I must like all types of cats.

## CARBONARA: WHAT IS ONE THING THAT ANYONE SHOULD DO BEFORE THEY DIE?

I haven't given much thought to such a question, so I don't have a good answer. I imagine that it would be more meaningful to come up with a LIST of things one should aim to do, and that such a list would be highly personalized. I am ripe for a midlife crisis, so perhaps its now time for me to compile such a list.

## SIGSEGV: WHAT ARE YOUR THOUGHTS ON RECENT PROGRESS IN QUANTUM COMPUTING, E.G. GOOGLE'S 72 QUBIT COMPUTER? COULD WE POSSIBLY SEE EFFICIENT FACTORIZATION USING A QUANTUM COMPUTER WITHIN OUR LIFETIME?

Please see my [profTHOUGHTS](#) article. And thanks for giving me the idea to write on post-quantum cryptography.

## STAPLED: MANY PEOPLE HAVE TROUBLE MEMORIZING NAMES; HOWEVER, YOU DO IT SPECTACULARLY WELL. DO YOU HAVE TIPS ON HOW TO MAKE PEOPLE'S NAMES STICK IN YOUR BRAIN?

Actually, I'm terrible at remembering names, and even worse at pronouncing the names that I do remember. To overcome these limitations, I download a very handy list of student WatCard photos and names from LEARN at the beginning of a course. I then make a concerted effort to have one-on-one conversations with as many students as I can, and then associate these conversations with their WatCard photos.

## SWINDLED: WHAT ADVICE WOULD YOU GIVE TO STUDENTS WHO ARE INTERESTED IN PURSUING CAREERS RELATED TO CRYPTOGRAPHY?

Most jobs that require expertise in cryptography fall under the category of "security engineer" or "cybersecurity professional". To prepare for such a job, it suffices to take a couple of courses in cryptography and security (including CS 458 -- Computer Security and Privacy), and general courses in computer science and mathematics. Most importantly, try to get an internship or two with a primary focus on cryptography or security. You can also boost your security credentials by taking online courses, acquiring CISSP certification, or doing a professional or research Master's in an area of cryptography or security.



# POST-QUANTUM CRYPTOGRAPHY

profTHOUGHTS 137.1

Quantum computers were conceived by Richard Feynman and Yuri Manin in the early 1980's. These devices exploit weird properties of quantum mechanics, such as superposition, to manipulate data in surprising ways. The fundamental element of a quantum computer is a *qubit*, which can exist in two states at the same time, each with a certain probability. An  $n$ -qubit register is a collection of  $n$  qubits that can be in  $2^n$  states at the same time, each with a certain probability. When a function is applied to an  $n$ -qubit register, it is simultaneously evaluated at all  $2^n$  states. However, one should not view a quantum computer simply as a massively parallel computer. Indeed, when the  $n$ -qubit register is "measured", it reverts to being in one of the  $2^n$  states according to its underlying probability distribution.

In 1994, Peter Shor discovered a very efficient algorithm for factoring integers  $N$ . More precisely, Shor's algorithm has running time  $O(\log N)^{2+\epsilon}$ , which is *polynomial* in the bitlength of  $N$ . In contrast, the fastest known algorithm for factoring  $N$  on classical computers has running time approximately  $O(e^{\log N^{1/3}})$ , which is *subexponential* in the bitlength of  $N$ . Thus, since hardness of factoring  $N$  is a necessary condition for the security of RSA, Shor's algorithm completely breaks the RSA public-key encryption and signature schemes. In fact, Shor's algorithm also completely breaks the other two families of public-key cryptosystems that are used today, including elliptic curve cryptosystems.

RSA and elliptic curve cryptosystems are widely used today to protect internet communications. For example, when you visit gmail.com, your browser negotiates a shared secret key  $k$  with Google's gmail servers using elliptic curve cryptography. Furthermore, RSA signatures are used to authenticate Google's elliptic curve public key, and therefore you are assured that your browser indeed shares  $k$  with Google (and with no one else). Thereafter, your communications with Google's gmail servers are encrypted and decrypted using  $k$ . If an entity were to capture and store these encrypted internet communications, and later have access to a large-scale quantum computer, then that entity would be able to compute  $k$  and thereby decrypt the communications.

This begs three questions:

1. When will large-scale quantum computers be built?
2. What, if anything, should be done to mitigate the threat?
3. When should action be taken?

## WHEN WILL LARGE-SCALE QUANTUM COMPUTERS BE BUILT?

The short answer is that no one knows with certainty.

In the past two decades, a lot of effort has been expended by theoretical and experimental physicists in designing and building quantum computers. UW's Institute for Quantum Computing (IQC) has been a leader in this effort. Large corporations such as IBM,

Microsoft and Google are also committing substantial financial resources to develop their own quantum computer prototypes. In November 2017, IBM unveiled a 50-qubit quantum computer. In March 2018, Google announced a 72-qubit prototype. Does this mean that the breaking of RSA and elliptic curve cryptosystems, and thus much of internet security, is just around the corner? The answer to this question is: likely not. IBM's and Google's quantum computers are comprised of 50 and 72 *physical* qubits, respectively. These qubits are inherently noisy because of "decoherence", and thus are stable for only a very short period of time. For example, IBM's computer can perform quantum calculations for only 90 microseconds, which would be insufficient for executing Shor's algorithm.

A quantum computer that can factor 2048-bit RSA numbers  $N$  (numbers of this size are commonly used in internet applications) would need a register of length at least 2048 qubits. These qubits would have to be *fault tolerant*, i.e., resistant to errors. Presently envisioned quantum computing architectures use specially designed quantum error correcting codes to combine several, perhaps thousands, of noisy physical qubits into one (essentially noiseless) *logical qubit*. Thus, *millions* of physical qubits might be needed to build a fault-tolerant quantum computer capable of factoring 2048-bit RSA numbers.

With this perspective, Google's 72-qubit machine would not appear to be an immediate threat to RSA or to elliptic curve cryptosystems. Indeed, no one has built a single fault-tolerant qubit to date. Some researchers believe that recent progress will eventually lead to the building of a fault-tolerant qubit, and then the challenge of combining many fault-tolerant qubits into a large-scale quantum computer will essentially be an engineering one. Nonetheless, it is extremely difficult at present to predict the rate at which progress will be made.

## HOW CAN THE THREAT BE MITIGATED?

Cryptographers have been working hard on developing public-key cryptosystems that, unlike RSA and elliptic curve cryptosystems, will withstand attacks by both classical and quantum computers. This area of cryptography is known as "post-quantum cryptography".

Two viable candidates for post-quantum cryptography are the following:

1. *Lattice-based cryptography*: Here the underlying hard problems are of the following flavour: Given  $n$  vectors  $v_1, v_2, \dots, v_n$  in  $Z_n$  that are linearly independent over the real numbers, determine a shortest nonzero vector in the lattice spanned by

the vectors, i.e.,  $L = \{ c_1 v_1 + c_2 v_2 + \dots + c_n v_n \mid c_i \in \mathbb{Z}_n \}$ .

2. *Isogeny-based cryptography*: Here the underlying hard problem is that of computing a map (given by rational functions) of a certain degree between two supersingular elliptic curves. This area of cryptography was pioneered by Luca De Feo and UW professor David Jao.

These candidates are relatively new, and thus need to be further scrutinized before one can have confidence that they will withstand attacks by classical and quantum computers in the decades to come. This task is complicated by the fact that there are very few researchers in the world who are experts in both quantum algorithms and in theoretical and algorithmic aspects of the underlying mathematics. Moreover, these quantum-safe candidates are relatively inefficient compared to RSA, and thus more research needs to be done on optimizing and implementing them to meet efficiency requirements of practical applications.

#### WHEN SHOULD ACTION BE TAKEN?

Under the cloud of uncertainty of the timeline for when large-scale quantum computers will become a reality, the U.S. government's National Security Agency (NSA) in August, 2015, released a major policy statement on the need for post-quantum cryptography. This announcement has served as a great stimulus to the development, standardization, and commercialization of quantum-safe cryptosystems. The U.S. government's National Institute of Technology (NIST) solicited proposals for quantum-resistant encryption and signature algorithms. A total of 69 submissions were received by the November 30, 2017, deadline from researchers around the world. These submissions will be carefully scrutinized by cryptographers in the next few years (indeed, some have already been broken). Among the survivors, NIST expects to select a small number of submissions for standardization after 5 years or so. In the meantime, large corporations and small startups are experimenting with deployment of quantum-safe cryptosystems in practical applications, and exploring ways to commercialize quantum-safe technology.

#### CONCLUSIONS

Post-quantum cryptography is now a vibrant research subfield of cryptography. The research subfield is inherently multidisciplinary in nature, drawing upon several disciplines of mathematics (e.g., lattice theory and elliptic curves), computer science, engineering, and quantum information theory. Progress, or lack thereof, on building large-scale quantum computers in the next few years will dictate the urgency with which quantum-safe cryptosystems will be deployed in practice.

Prof. Alfred Menezes

## MEF SEZ

Hello everyone! I've got some updates for you from your friendly neighbourhood endowment fund!

#### FUNDING PROPOSALS

tl;dr: we are MEF. you want monies? give us reasons. ty.

Group funding proposals for the Math Endowment Fund (MEF) are now open! Proposal forms can be found at <https://tinyurl.com/mef-proposal> or outside the ~~free-candy room~~ MathSoc office (MC 3038) and are due on **June 22 at 5pm ET**<sup>1</sup>.

Have you been dying to attend a hackathon, case competition, or conference, but couldn't because the price to attend was too high<sup>2</sup>? You may be able to receive up to \$750 in funding through professional development funding!. These proposal forms can be found at <https://tinyurl.com/mef-professional>. There's no due date for professional development funding, but they are **first-come, first-served**, so get your proposal forms in!

#### FUNDING COUNCIL NOMINATIONS

tl;dr: rep your year/program. give out \$175k. get free food.

Want to have a say in how over \$175,000 is spent? Join the funding council! We're looking for year reps (3 reps per year) and program reps (2 reps per program)<sup>3</sup>. This is a low-commitment position and will only require you to attend 2 evening meetings in early July. Also, free food that will most likely not be pizza<sup>4</sup> (unlike a certain fortnightly publication). More info about funding council, including nomination forms, can be found at <https://tinyurl.com/mef-council>. Forms can be also found outside the MathSoc office. Nomination forms are due on **June 15<sup>th</sup> at 5pm ET**.

Submit all forms to the MathSoc office or email them to me at [mefcom@uwaterloo.ca](mailto:mefcom@uwaterloo.ca).

If you have any questions (or want free sticky notes and laptop stickers<sup>5</sup>), feel free to send me an email!

Have a great term!

Alex Lee  
Executive Director, Spring 2018  
Math Endowment Fund

1. 4pm Central Time, 2 pm Pacific Time, 11pm Central European Summer Time.
2. Insert "too damn high!" meme here.
3. Including CFM and Software Engineering!
4. No guarantees.
5. I'm being serious.

## profQUOTES 137.1

### CS 343: PETER BUHR

“ We can go back to the hardware engineers and ask "Do you have Assignment 4 Question 2 instructions".

### CS 450: ANDREW MORTON

“ I've gone too long. I've taken up too much of your time. I'm going to leave now.

“ As an undergrad, we never had this many [practice exams]. We had to walk to school uphill both ways.

“ Have a happy life and all that.

“ [Just before the exam] I'm going to sit at the back and work on the solutions.

### CS 487: ERIC SCHOST

“ One of your inputs is a Tetris brick, so we have to fix that.

### MATH 146: MATT KENNEDY

“ I told you this proof is two lines... where 2 equals 10.

### STAT 341: REZA RAMEZAN

“ I don't want to get political but next year we are all going to freeze. Princess Elsa will come in and Santa Claus will be moving in!

### STV 210/HIST 212: SCOTT CAMPBELL

“ [Tells a joke]  
[Silence from class]  
That was like my best bad joke! Let's try this again:  
[Says punchline of joke again]  
[Still silence]  
Okay, we're going to have to deconstruct this.

“ "Sure he hasn't read Dickens, but how many of you know the Second Law of Thermodynamics?" I know, sick burn, right?

“ "Half-assed" doesn't really work because it's a fox.

“ I'm going to put [my phone] down, I'm going to class and I'm not going to look at it. *Hint hint.* That was a joke.

### PSCI 369: DAN GORMAN

“ Why do I bring [the Soviet boycott of the UN Security Council] up? Because it seems some of your peers are boycotting these lectures.

### HIST 216: IAN MILLIGAN

“ I can make false promises now that you've done your course evaluations.

“ [For the exam] I told the registrar: "I want a two-hour time slot and I want it in RCH because I'm busy." I got neither.

“ We're not looking for grammar—well, don't be an idiot.

## N TIPS FOR SURVIVING A WARM, SUNNY SPRING DAY

- Drink lots of water and carry a reusable water bottle.
- Carry sunglasses to prevent eye damage.
- Make use of indoor tunnels and bridges to avoid happy couples enjoying the weather, who will block your path and slow down your commute.
- Dress in layers to block out as much of the sun as possible.
- If you can't dress in layers, use sunscreen to protect your skin.
- Sunscreen can contain dangerous chemicals. Avoid showering instead to shield your skin with an all-natural thick layer of dirt.
- Windows lead to contact with the sun. If your lecture hall has windows, attend a later lecture which will either not have windows or be so late that the sun has already set. If there are no such lectures, skip class and come back on a rainy day.
- Do not go to class on rainy days. Rainwater will stick to your skin and act as a magnifying glass for the sunlight—not to mention washing away your protective dirt.
- Avoid visiting your professors during office hours. More likely than not, their office will have windows.
- Do not go to your exams if they are scheduled in PAC - the indoor path from SLC has windows.
- Use Linux, because something something Windows.

AC

## A SUNNY REMINDER

Wear some damn sunscreen  
'Til the white cast can't be seen  
Your skin will thank you!

Canadian Dermatology Association

## WHAT IS AN ACTUARY?

The world of Actuarial Sciences is a critical piece of the insurance industry, and many people over the past decade have been taking greater interest in this applied sibling of statistics. As such, I, an ActSci student, have often been asked "What is an actuary?" And today, I would like to set the record straight and answer this question. Prepare yourselves.

The main title to remember when thinking of an actuary is "risk management specialist." Effectively, actuaries are responsible for determining and managing the risks of offering insurance. This includes pricing insurance and financial products and setting the reserves a firm holds.

As for the techniques an actuary uses to achieve these tasks, the main source is dark magic – but actuaries have also been known to dabble in geomancy and divination. Sacrifices are made regularly from among the less educated of the Sorcerers' Order of Actuaries (SOA), although the Canadian Insurance Arcanum (CIA) also provides some sacrifices.

Speaking of the actuarial societies, there are generally two levels of expertise. First, we have the associate level (ASA and ACIA), which are actuaries who have completed the first set of exams, commonly referred to as the "preliminaries", required for proving their competence in the subject matter. Next we have the fellow level (FSA and FCIA), which are actuaries who have completed a more advanced specialization within Actuarial Sciences. An important note: fellows of the actuarial societies are the only individuals technically considered to be "actuaries", with the associate and pre-associate levels being referred to as "actuarial associates" and "actuarial students" respectively.

Regarding the examination process to achieve these designations, budding actuaries are thrust head-first into a hellish series of examinations from which fewer than half of all candidates survive. The adjustment to the arcane arts is not kind to all, and many fresh faced students come out of the process jaded, sadistically enjoying the suffering of the people who follow in their footsteps. Once finished the trials, actuaries find themselves with much time on their hands, allowing them to pursue new magical and foul hobbies, such as necromancy or accounting.

Overall, actuaries are very important to the continuation of insurance industries in Canada. I hope this has been informative, and remember: donate blood often. Actuaries need strength.

New&Confused

Send more profQUOTES.

THE ENTIRE mathNEWS READERSHIP

## MEATLOAF AND WORKING FOR IMPRINT

### HE CERTAINLY WOULDN'T DO THAT FOR LOVE

It's been often asked on forums what Meatloaf is referring to in his hit song *I'd Do Anything For Love* that came out in 1993. Meatloaf himself claims that the lyrics are meant to be ambiguous, but when I have a hunch that there may be hidden meanings within a piece of artwork, I must investigate.

### A BRIEF HISTORY OF STUDENT NEWSPAPERS AT UW

While some may know *The Chevron* as an "edgy" underground newspaper at present, it was once the official student paper of UW. *Imprint* replaced *The Chevron* in 1977.

Interestingly enough, Meatloaf's rise to fame occurred in the same year, with his rock opera album *Bat Out Of Hell* reaching platinum status. This, metaphorically, represents the shift of student newspapers at UW: The bat (*The Chevron*) escaping the hell that is Feds censorship, in which the void of hell is filled with *Imprint*.

Almost a decade and a half later, *Imprint* is looking to expand their icy grip on campus. Likely, they contacted Meatloaf to do a charity gig to raise funds for *Imprint*. While Meatloaf loves knowledge and journalism, Meatloaf would do anything for love, *but he won't do that*.

Vice Mitt

## FLAT EARTH EDGE-FALLING-PROTECTION INSURANCE

Policyholders are insured against death due to falling off the edge of the planet.

Benefits will be paid to the sum of \$40,075, in the event that an independent investigation can prove that the cause of death was falling off the edge of the Earth. Premiums will be set at \$314 per year.

Policyholders will have access to a comprehensive database of modern and historic scientific publications indicating the round nature of planet Earth.

Policyholders may lapse on their policies at any time, but return of premium is not offered for this product.

New&Confused

## AN SHORT BRAINFUCK TO C TRANSPILER IN C

```
#include <stdio.h>
int main( void ) {
    printf( "#include <stdio.h>\n" );
    printf( "int main( void ){ " );
    printf( "char array[30000]; int p = 0;" );
    for( char c = getchar(); c != EOF; c = getchar() ) {
        switch ( c ) {
            case '>' : printf( "p++;" );
            case '<' : printf( "p--;" );
            case '+' : printf( "array[p]++;" );
            case '-' : printf( "array[p]--;" );
            case '.' : printf( "putchar(array[p]);" );
            case ',' : printf( "array[p]=getchar();" );
            case '[' : printf( "while(array[p]){ " );
            case ']' : printf( "}" );
        }
    }
    printf( "}" );
}
```

+[]

## N SIGNS IT'S ACTUALLY NOT WINTER ANYMORE!!

### GLORIOUS, GLORIOUS WEATHER!!!!

- There is actual, distinct colour in the world outside other than snow white.
- There is an outside that you can easily explore now!
- Baby geese are exploring the campus (beware their angry parents though!)
- More people who are outside have... their skin... actually visible...
- The scent of the neighbouring farmland can actually be smelled.
- The clock has seeeeeeeeeeemingly been reset for snow days, so we're back to probably not having any more until 2023 based on Drowning in Cocoa's estimates. (see [mathNEWS v136i1](#))
- There's a humidex value associated with the temperature forecasts now; not to mention the ultraviolet ray index from the sun... because that ALSO exists!
- There is air-conditioning in more rooms on campus than just M3 1006!
- The proto-frosh are starting to evolve into pre-frosh!
- I am no longer wearing TWO pairs of pants every day to keep out the cold (still need a hoodie for that air-conditioning though...)

waldo@<3.LE-GASP.ca

## COMPANY INNOVATES PRODUCT LAUNCH BY ACCIDENTALLY LEAKING PRODUCT

Disaster struck for Amazing Software Inc. last night. The source code for their new prototype, titled "Dysruptr" was leaked by a disgruntled intern, exposing what journalists had already suspected about the barely known product - that the company has absolutely no idea what they're doing.

"This is truly a milestone in my life," said Dirk Hasselton, the man whose 5 non-YouTube-related hours of work per week were almost singlehandedly responsible for an undocumented mess of code which barely functions, and which everyone in the office is afraid to ask about. "I feel like I contributed a great deal to this product, and I'm expecting a raise in the near future."

"What we are seeing is an unprecedented revolution in tech development," added journalist Cayden Bennett. "This thing doesn't even come close to compiling, and any meaningful data is wrapped in an endless string of references and pointers. The use of single letter variables throughout the 20000 line program makes for the most unreadable piece of garbage I've ever seen in my 19 years of reporting here."

Managers were left just as confused as the public as to the meaning of this heaping mess. General manager Shawnda Julyan gave comment: "Nobody really knows what this thing does, or even if it does anything. Upper management assured us that it's something related to machine learning, but nobody at the office knows any machine learning. Heck, half of them don't even know how to program. Two of these guys just come in to play ping pong for seven hours with a one hour lunch in between."

Recent reports confirmed that the company was using their agile methodology to pivot away from Javascript in favour of PHP, in order to further optimize the unreadability of their code. Jess Kaufman, lead web developer, spoke on the issue. "Well, if we can't make any dollars from the software, we'll at least have tons of dollar signs within the code itself. That should please management."

The CEO unfortunately could not be reached for comment as he was reportedly "in the middle of a VR match so shove it, loser." Further details will be published as they arrive throughout the week.

NitricAcid

## N THINGS TO DO WHEN YOU CAN'T THINK OF A TOPIC FOR A mathNEWS ARTICLE

- Panic
- ~~Resort to meta~~
- Whine about not having ideas
- Whine about not having ideas again, but louder this time
- Ask people for ideas cause they're not picking up on your subtle hints
- ~~Resort to meta~~
- Look at recent news
- Look at recent memes
- Think of all your embarrassing memories that could be exploited for **mathNEWS** articles
- Rip the first 50% of your hair out
- Panic again
- ~~Resort to meta~~
- Consume industrial amounts of caffeine
- Rip the remaining 75% of your hair out
- Perform blood sacrifices to appease the **mathNEWS** editors
- Come to the conclusion that everything you have ever done in your life is a failure
- Feel yourself being crushed by the infinite weight of your sheer insignificance
- Let your sanity slip into the void as you embrace the all powerful darkness
- Resort to meta

Various Pseudonyms

## SLIDING IS COOL

Evidence:

- Sliding into those DMs
- Penguins and seals slide around
- Slip-n-slides
- Grinding on a skateboard is just fancy sliding
- Slideshows (cool if you teach grade 5)
- Snowboarding is also complicated sliding with jumping mixed in
- Sliders (the cute little burgers)
- Ice is slippery and very cool, almost cold
- The Electric Slide
- Sliding down a fire pole is what firefighters do, and their job is to cool down the average temperature of things
- Slide whistles (cool if you're a dad)
- Actual slides

Diminutive Rex

## N THINGS NOT TO DO WHEN RUNNING A STATISTICAL STUDY

- Unintentionally harm your subjects.
- Organize your experiment to be single blind by only telling the subjects which treatment plan they are on, not the administrators.
- Refer to the subjects as "sacrifices".
- Intentionally harm your subjects.
- Promise compensation in the form of sweaty handshakes.
- Include obvious outliers in the final model because "they were trying their best".
- Ignore the error term because you wanted to play connect the dots.
- Promise compensation in the form of copies of Imprint.
- Hold uncooperative survey subjects at goose-point.
- Choose subjects based on their creativity when answering the question "What's the best way you can think of to introduce uncontrollable bias to this study?"

New&Confused

## N STEPS TO WRITING A mathNEWS ARTICLE

- Have an idea
- "No, that's stupid"
- Write it anyway to fill space

New&Confused

math news



**ACTSCI:** After writing your first actuarial exam, you were overcome with a certain apathy that you just couldn't seem to shake off. Study this and that for  $X$  hours and you'll pass. Right? That's all your life has come to, the bitterness of cramming your head with modules every night while everybody is having fun without you. Is that all there is to life, studying for exams and biting your nails away waiting for your exam results to just move on with your career? Your life has become binary and you can't see a way out. Is there anything more than money and making rich corporations richer?

Ah, you shake your head and continue studying for your next upcoming exam this weekend. No point in philosophizing, you say. It's too late to change majors now.

Your unlucky number is: Any number greater than 400. Those 400+ hours you could have spent having fun instead went into studying for exams.

**AMATH:** To further your understanding of PDEs, you decide to attend a graduate seminar. You are disappointed to find out that the speaker isn't interested in solving the equation, but to prove that given certain conditions about the function space the boundary condition is in, one can bound the norm of the wave operator in some other function spaces. You leave more confused than ever.

Your unlucky number is:  $(2, 2, \infty)$ . The one thing you remember from the talk is this triple, which was some sort of counter-example to something you didn't quite understand.

**Bioinformatics:** Finally, you landed a much coveted research position with a rural medical clinic. Your very talented supervisor splits his time between research and practicing medicine for the local community. The work is interesting and you are surrounded by pristine nature. For the long weekend, you decide to go on a camping trip.

Your unlucky number is: Oops, you only brought 3 tissues for the whole weekend. You make do with some leaves which cause an unbearable rash by Tuesday. As the only doctor in the community, your supervisor makes small-talk as he confirms that your butt rash is caused by poison ivy.

**C&O:** You signed up to run a work shop to motivate kids to like math. You decide it would be a great idea to have them split into two teams, Russia and USA, to demonstrate an interesting optimization problem. Russia's task is to find out how much wheat they can move across the country on their railway network, while USA's task is to find out how many bombs they need to cut off the entire supply of wheat.

Your unlucky number is: 30 kids who like war more than math.

**CS:** The new Amber Alert system sucks! You think it's really badly implemented and that it has the potential to cause more harm than good by crying wolf. Unfortunately, they cannot be silenced on your phone, so a temporary measure, you disable emergency alerts.

Your unlucky number is: 0 warnings of imminent tornado threat.

**FARM:** You feel terribly misunderstood. No one knows what FARM is except for your fellow FARMers. When meeting new friends at Bomber, they assume you're in environment because what the heck is farm? A new innovative major in the environment faculty? Deep down, you're hurt, but you laugh and drown your sorrows in cheap, watered down Jägerbombs.

Your unlucky number is: 10 tears you cry each moment someone asks what FARM is.

**Grad:** Congratulations! You get to teach a course this semester! What better way to spend an entire semester than by motivating inquisitive young minds on the questions that lead you to pursue research?

Your unlucky number is: 2.5 times the salary of a regular TA for 7 times the work.

**PMATH:** Ever since first year you've heard so much hype about modular forms, the Weierstrass P-function, and Riemann surfaces. You are excited to finally learn the theory behind all these concepts and appreciate the beauty of it all.

Your unlucky number is: 352 is about plotting curves and contest problems.

**Software Engineering:** Your favourite colours are purple and pink, but when pressured to choose, you most certainly say purple. Engineering's not a cult, right? That's what you like to tell yourself as you drink a beer with your cohort friends in POETS and discuss the ranking of the Big 4 (or is it 5?) software companies. Lucky you! Math is for squares, anyway.

Your unlucky number is: 40 for the number of jobs you applied to and the interviews you received.

**STAT:** One of your instructors is a handsome oppa with a classy af accent. You start going to lecture more regularly to see him. You notice your grades improving.

Your unlucky number is: He's a solid %0.

# ZETHAR, SIGNING OFF

It has come to this.

I mean, I've always known that it'd happen sooner or later: the editors finally are fed up with my shenanigans and want to be able to sleep at night without worrying about disgruntled **gridWORD** solvers putting a hit on them when they expected it least. They've found someone to oust me from this iron throne and actually make good crosswords with a consistent theme. No, I'm not bitter; after all, it's been a pleasure and the bonus of watching George run up and down panicking has been worth it, but alas, nothing is eternal for the unceasing march of temporal progression heeds no being, and it is better for **mathNEWS** as a whole if fresh blood rises to claim this damnèd throne lest I wither and die upon it with no contingency. You, dear **gridWORD** solvers, have much to look forward to (for I have seen some preliminary work of my successor), while I fly into the sunset beyond. I might occasionally drop by with regular articles, but for now, this might as well be farewell—at the very least, from this post.

Worry not, for **gridWORD** marches on: one shall not let such a grand tradition lapse at the mere inconvenience of a transition. I invite the solvers, new and old, to join me once more while I document a full version of the **gridWORD** boilerplate so even in my absence this column shall trudge along unimpeded, stalwart as it has always been:

- Solvers to the issue's **gridWORD** may elect to submit their solution to **mathNEWS**, wherein the most correct solution shall be awarded a prize by the **gridMASTER**.

- For a solution to be eligible, it must be submitted either physically to the **BLACK BOX** (located outside the Math C&D; please refer to the pictures in volume 136, issue 5 for more details) or electronically to [mathnews@gmail.com](mailto:mathnews@gmail.com) with names of solvers (and optionally, a moniker of which the solution is to be credited) by 1800 hrs on the date of the production night of the next issue in the term (in this case, May 28<sup>th</sup>, 2018), provided it exists.
- In the event of a tie for most correct, the **gridMASTER** makes a selection among the answers which are most correct, of which the traditional method is the **gridMASTER**'s favourite answer to their **gridQUESTION** of the issue. (Traditionally, it is described as "funniest" but in practice, it's "whatever the **gridMASTER** likes the most" so in the interest of transparency...)
- If one is listed as having won the prize of the issue, one may drop by the **mathNEWS** office to pick up the prize. Please bring your Watcard or some other form of identification which matches the name of the submission (which might be different from the moniker it is credited to—it gets sorted out via administrative magic)

With that in mind, I shall pose this issue's **gridQUESTION**, of which shall be the tiebreaker question for my **gridWORD**, to be judged by my successor: "What is some advice you would like to offer to the incoming **gridMASTER**?"

Signing off,

Zethar  
gridMASTER v131i3 – v137i1



## 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](mailto: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.

1	2	3	4		5	6	7	8		9	10	11	12	13
14					15					16				
17				18						19				
20								21	22					
			23				24							
25	26	27				28			29			30	31	32
33				34				35			36			
37			38			39				40				
41					42				43			44		
45				46			47				48			
			49			50			51					
52	53	54							55			56	57	58
59						60	61	62						
63						64					65			
66						67					68			

**ACROSS**

- 1 . Check
- 5 . Swiped
- 9 . Listing
- 14 . Taxi alternative
- 15 . Rajah's mate
- 16 . Horsemen's exhibition
- 17 . Enjoyed
- 19 . Angler's basket
- 20 . Hazing prank
- 21 . Serpent
- 23 . Legend on the ice
- 24 . Salk's study
- 25 . Wield
- 29 . Consolidates
- 33 . Listening device
- 34 . Flowering
- 36 . Acid + base product
- 37 . Striped beast
- 39 . Dark time for poets
- 40 . Ghostlike
- 41 . Lepton's locale
- 42 . Sun shade
- 44 . "To Autumn," e.g.
- 45 . Ring bearer?
- 47 . Recurred
- 49 . Typesetting system
- 51 . /

- 52 . Dress
- 55 . Nagana carrier
- 59 . Ring-tailed animal
- 60 . Iniquity
- 63 . "The Waste Land" poet
- 64 . Warner Bros. creation
- 65 . Paper abbr.
- 66 . Canadian pastime
- 67 . Border
- 68 . Offenses

- 18 . Anglo-Egyptian Army commander
- 22 . Grad
- 24 . Solar bird
- 25 . Trial versions
- 26 . Yogurt dish
- 27 . Cant
- 28 . Multitude
- 30 . French game
- 31 . Leave out
- 32 . Charger
- 35 . "Step \_\_\_!"
- 38 . Impersonation expert
- 40 . Exit
- 42 . Chip in
- 43 . Poseidon
- 46 . Blue moon, e.g.
- 48 . Stops
- 50 . Select
- 52 . Top guns
- 53 . Italian traveller
- 54 . Poker holding
- 56 . South American monkey
- 57 . Look over
- 58 . Sushi fish
- 61 . Silent assent
- 62 . Nudge

**DOWN**

- 1 . Syndicat des travailleurs et travailleuses des postes
- 2 . Qualified
- 3 . Kind of instrument
- 4 . 
- 5 . Sternum attachment
- 6 . Row
- 7 . An identity
- 8 . Buddy
- 9 .  $\int (1+x^2)^{1/2} dx$
- 10 . Race winner
- 11 . Inkling
- 12 . Move that decreases opponen's defense
- 13 . Ratted

## A PUBLIC BROADCAST FROM YOUR NEW puzzleMASTER IN CHIEF

haltingCOMMENT 137.1

Greeting **mathNEWS** readers, puzzle addicts, **EDitors!** Long time reader, first time poster. I was recently approached with an offer for the esteemed position of **mathNEWS puzzleMASTER** for the term, and I was just blown away. How could I turn down such an honour? How indeed. But that is not our puzzle today! Starting today, and for the next six weeks, I will present for you, dearest **puzzleSOLVER**, a Masyu puzzle! Perhaps you've heard of them before, perhaps not—but they're some of my favourite to solve.

The goal of a Masyu puzzle is to draw a single loop, with lines going from box to box, though not necessarily every single one. There must be only one single, finished loop, and it isn't allowed to touch or cross over itself. The black and white circles dictate what the loop must look like.

**Black circles** indicate corners, and the loop *must* make a turn in the square with the black circle. Furthermore, in each of the squares where the loop extends from the corner, it *may not* make a turn. So, at a black square, the loop makes a turn and extends straight out a full square.

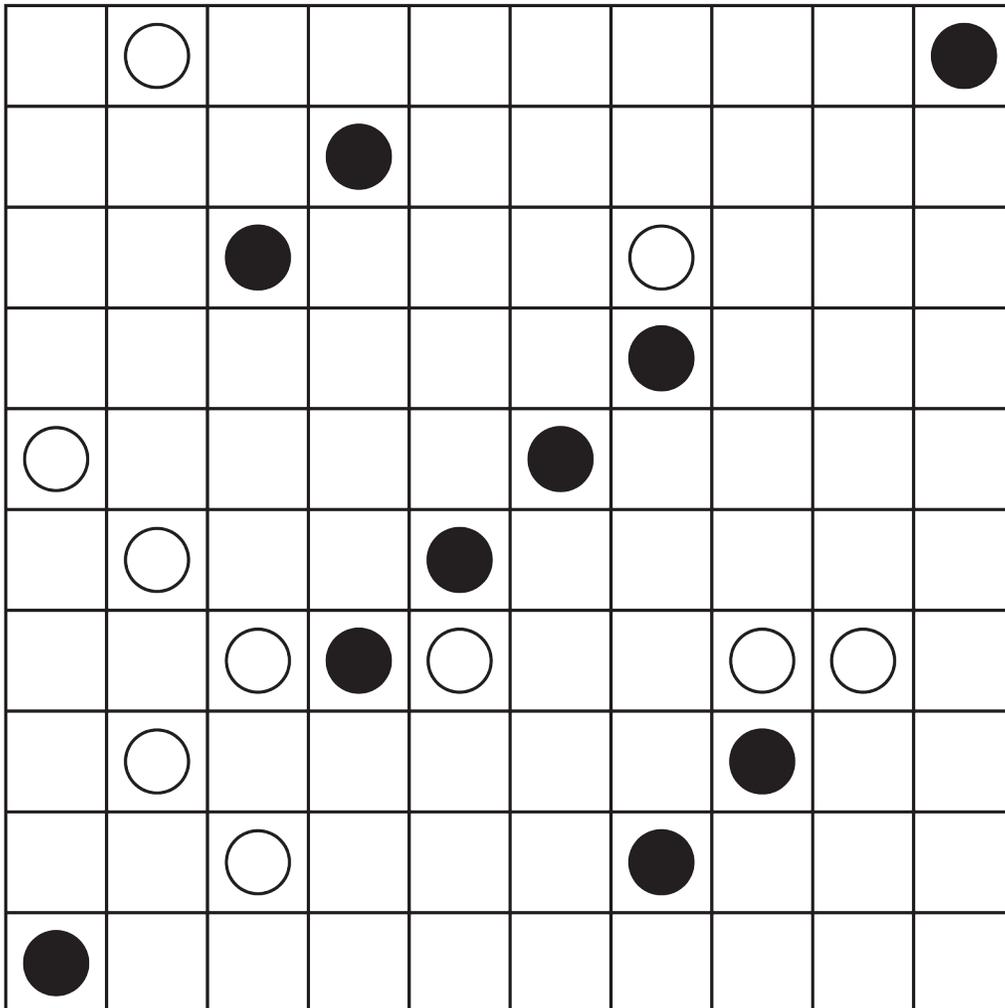
**White circles** indicate straights, and the loop *may not* make a turn in the square with the white circle. Furthermore, the loop *must* turn in one, or both, of the squares where the loop extends from the straight. So, at a white square, the loop passes straight through and then turns in one adjacent square.

And that's it! There's a few more common tricks to figure out, but I'll leave that to you, dear **puzzleSOLVERS**. Or, you can read some more comprehensive tutorials online.

goodLUCK!

<https://krazydad.com/masyu/tutorial/>

The puzzleMASTER



# lookAHEAD

SUN MAY 20

MON MAY 21

Victoria day  
(university holiday)

TUE MAY 22

Make up for Victoria day  
(Monday schedule)

Drop no penalty period  
ends (last day to drop  
with 100% refund)

WED MAY 23

Drop penalty period 1  
begins

THU MAY 24

Final exam schedule  
released

FRI MAY 25

SAT MAY 26

SUN MAY 27

MON MAY 28

mathNEWS 137.2  
production night

Co-op interviews begin

TUE MAY 29

Intranational bring ice  
cream to the mathNEWS  
editors day

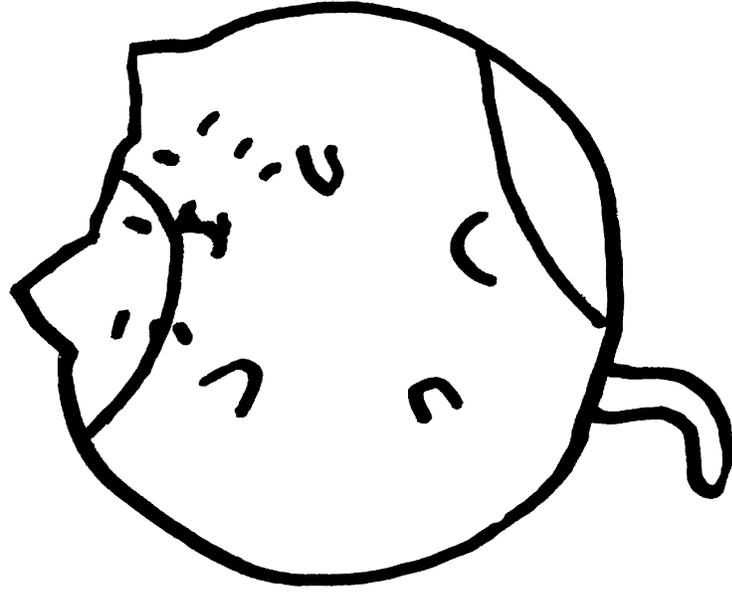
WED MAY 30

THU MAY 31

FRI JUNE 1

SAT JUNE 2

mathNEWS 137.2  
published



## mathNEWS SEZ

Come to production night!

As great as Spring term is, one unfortunate side effect is that not as many people come to mathNEWS production night. That makes us editors sad. We have all this free pizza to give away, but no friends to share it with. The more articles we have, the less you'll hear the editors whining about it.

swindLED

## A mathNEWS HAIKU

Ah, production night  
Please come to production night  
We have free pizza!

itorED

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