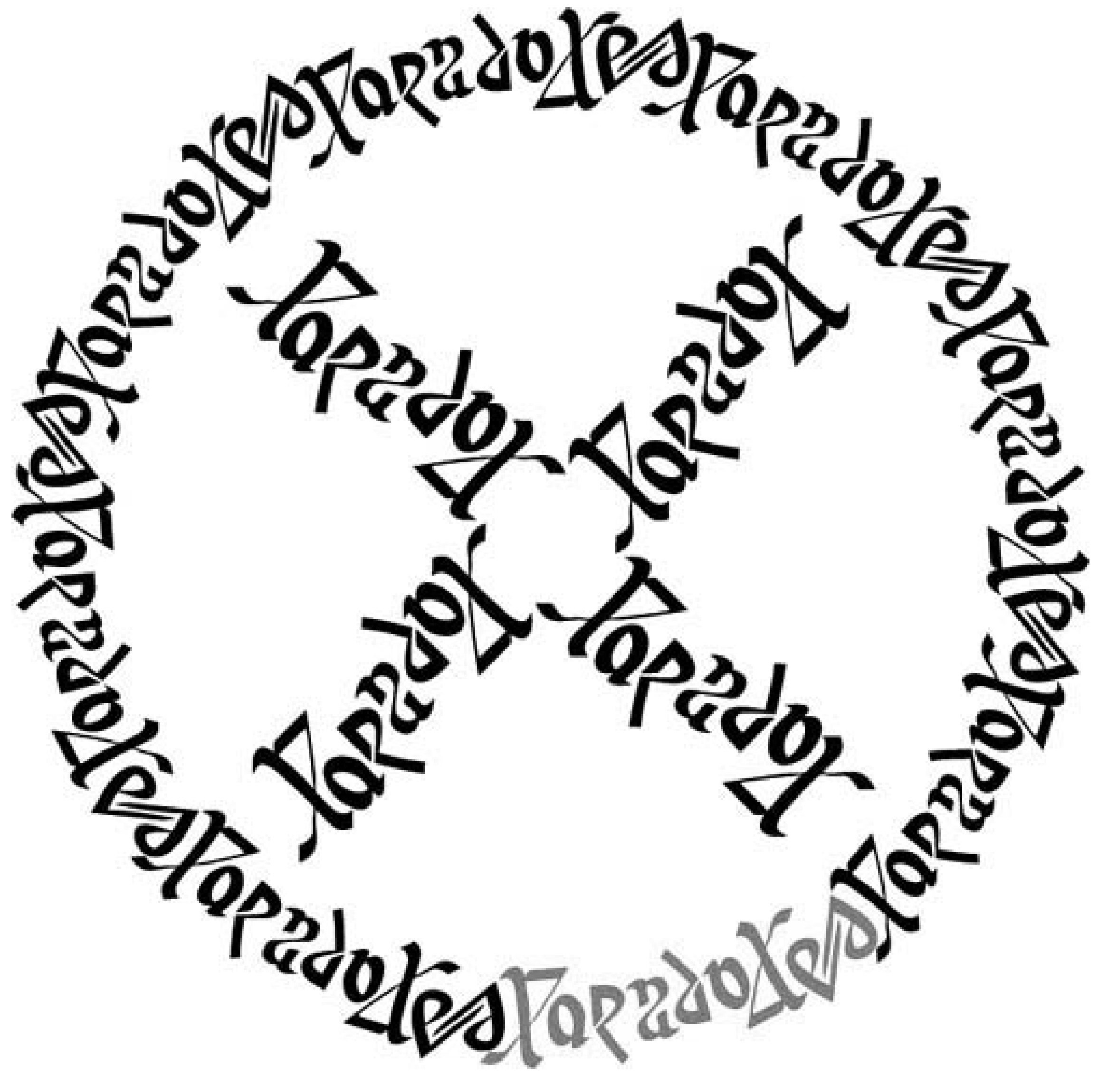
Paradox

Issue 1, 2004

The Magazine of the Melbourne University Mathematics and Statistics Society



MUMS

President:	Damjan Vukcevic d.vukcevic@ugrad.unimelb.edu.au
Vice-President:	Geordie Zhang g.zhang@ugrad.unimelb.edu.au
Treasurer:	Andrew Wee a.wee@ugrad.unimelb.edu.au
Secretary:	Nick Sheridan n.sheridan@ugrad.unimelb.edu.au
Education Officer:	Maurice Chiodo m.chiodo@ugrad.unimelb.edu.au
Publicity Officer:	James Saunderson j.saunderson@ugrad.unimelb.edu.au
Editor of *Paradox*:	Norman Do norm@ms.unimelb.edu.au
1st Year:	Andrew Kwok a.kwok2@ugrad.unimelb.edu.au
2nd Year:	Julian Assange j.assange@ugrad.unimelb.edu.au
3rd Year:	Alex Feigin a.feigin@ugrad.unimelb.edu.au
Honours:	Paul McCormick paulhm@ms.unimelb.edu.au
Postgraduate:	Daniel Mathews dan@ms.unimelb.edu.au
Web Page:	http://www.ms.unimelb.edu.au/~mums
MUMS email:	mums@ms.unimelb.edu.au
Phone:	(03) 8344 3385

Paradox

Editor:	Norman Do
Subeditor:	Nick Sheridan
Layout:	Stephen Farrar
Web Page:	http://www.ms.unimelb.edu.au/~paradox
E-mail:	paradox@ms.unimelb.edu.au
Printed:	April, 2004

Words from the Editor...

Welcome to the first issue of Paradox for 2004! For the uninitiated, this magazine that you hold in your hands is a publication brought to you by MUMS, the Melbourne University Mathematics and Statistics society. For the more experienced reader, I can assure you that this issue is as action-packed and hilarious as ever.

This particular Paradox contains articles on the RSA challenge and art gallery theorems as well as an interview with mathematician Craig Hodgson. As always, there are also a few maths problems for you to try your hand at for cash prizes. Our resident comic strip hero, Knot Man, is also back from a much needed holiday and this issue sees him battling with new enemies in The Matrix! And, of course, there are various maths jokes scattered throughout for you to laugh and/or groan at!

I hope that you all enjoy reading this issue of Paradox and have a great first semester. I encourage you to partake in MUMS events, such as the free barbecue and trivia competition which will be coming up after the Easter break. If you have any queries, comments, or wish to submit mathematical jokes and articles, please feel free to e-mail me at `paradox@ms.unimelb.edu.au`.

— Norman Do, Paradox Editor

...and some from the President

Welcome to 2004, and for the new students out there, welcome to MUMS!

For those who haven't yet heard about us, we are a student club for maths and stats students, and for anyone who is interested in the fun side of mathematics. We run a range of social, competitive and educational events throughout the year including trivia nights, free barbecues, regular seminars, and our infamous Maths Olympics (a crazy competition designed to stretch your athletic and cognitive abilities to the limit) which are held in semester two. We also publish Paradox! Yes, that's the magazine you are reading right now. Like our seminars, its aim is to display some interesting mathematics, in an informal and entertaining way.

Soon after the Easter break, we will be holding our AGM — this is where you get to elect a new committee for MUMS. I encourage all of you to come along and vote (did I mention there will be free pizza?), and even consider nominating yourself for a position. Being on a committee is the best way to get really involved in a club, and meet lots of new people along the way!

O-Week saw a very successful MUMS BBQ, and we hope to repeat that performance later in the semester. Also, we will be running a trivia competition towards the end of May. Watch out for these events!

— Damjan Vukcevic, President of MUMS

Front Cover

The front cover of this issue of Paradox is an example of what is known as an ambigram. Ambigrams are a particular type of visual wordplay in which a word or phrase is written so that it possesses some sort of symmetry. For example, each instance of the word "Paradox" on the front cover has been written so that it looks exactly the same when turned upside down.

The ambigram appearing on the front cover was drawn by Punya Mishra. Many thanks go to him for allowing us to use some of his fine artwork, much more of which can be seen at

`http://punya.educ.msu.edu`

A Mathematician, an Engineer and a Physicist. . .

A mathematician and an engineer are sitting in a lecture by a physicist. The topic concerns Kaluza-Klein theories involving physical processes that occur in spaces with dimensions of nine, twelve and even higher. The mathematician is clearly enjoying the lecture while the engineer is frowning and looking confused and puzzled. By the end, the engineer has a terrible headache whereas the mathematician comments about the wonderful lecture.
Engineer: "How do you understand this stuff?"
Mathematician: "I just visualize the process."
Engineer: "How can you visualize something that occurs in 9-dimensional space?"
Mathematician: "Easy! First visualize it in N-dimensional space, then let N go to 9."

One day a farmer called up an engineer, a physicist, and a mathematician and asked them to fence off the largest possible area of land with the least amount of fencing. The engineer made the fence in a circle and announced that he had the most efficient design. The physicist made a long, straight line and proclaimed, "We can assume the length is infinite. . . " and pointed out that fencing off half of the Earth was certainly a more efficient way to do it. The mathematician just laughed at them. He built a tiny fence around himself and said, "I declare myself to be on the outside."

A mathematician, a physicist, and an engineer were travelling through Scotland when they saw a black sheep through the window of the train.
"Aha," says the engineer, "I see that Scottish sheep are black."
"Hmm," says the physicist, "You mean that some Scottish sheep are black."
"No," says the mathematician, "All we know is that there is at least one sheep in Scotland, and that at least one side of that one sheep is black!"

An Interview with Dr Craig Hodgson

Our very own Dr Craig Hodgson, a senior lecturer in the Department of Mathematics and Statistics, has recently been awarded the Faculty of Science Dean's Award for Excellence in Research. I was fortunate enough to be slotted into his busy schedule and given the chance to find out more about the man and his work.

> "I am interested in the geometry and topology of 3-manifolds — objects that look locally like three dimensional space."

I must have looked a little puzzled, so out came the educator in Dr Hodgson (as well as pen and paper).

> "If you take a surface, such as a sphere, and zoom in on it, it looks like like a plane — 2 dimensional space. A 3-manifold has the analogous 3 dimensional property... These objects are important as they give a model for the space in which we live. Work in this area is especially of interest to physicists and cosmologists who are currently investigating the topology of the universe."

Some of Dr Hodgson's most recent work is closely related to Thurston's Geometrisation Conjecture, arguably the (as yet unscaled[1]) pinnacle of this area of mathematics. Indeed Dr Hodgson completed his Ph.D. at Princeton University under William Thurston, himself a Fields medalist[2].

When I discovered this I started to realise just how outstanding my 620-233 lecturer really is.

Dr Hodgson's interest in mathematics is long-standing. He recalls:

> "I guess I was interested in mathematics from primary school onwards... I used to borrow all the maths books from the local library when I was at school."

[1] The Russian mathematician, Grigory Perelman, claims to have a proof of Thurston's Geometrisation Conjecture, and with it the million dollar Poincaré conjecture, but it is yet to be verified.

[2] The Fields Medal is the mathematical equivalent to a Nobel Prize.

Dr Hodgson went on to undergraduate study at the University of Melbourne. He recalls a number of current staff members from his student days including Professor Chuck Miller, and his now next-door-neighbour on the first floor of the Richard Berry Building, Dr John Groves. Of the current Head of Department he noted,

> "Hyam Rubinstein appeared when I was in about 3rd or 4th year. He was quite an inspiration."

Dr Hodgson went on to complete a Masters under Professor Rubinstein before heading off to Princeton.

After nearly a decade in the U.S. at Princeton as well as other prestigious institutions such as the Mathematical Sciences Research Institute at the University of California Berkeley, and Columbia University in New York, Dr Hodgson ended up back in Melbourne.

> "... It's a great place for low dimensional geometry and topology... The students here are excellent."

Beyond academia Dr Hodgson has a diverse range of interests.

> "I do a lot of bushwalking. In December I went to the South Island of New Zealand. I also regularly go on trips throughout Victoria and Tasmania.
>
> "I am also interested in music. I play the piano, bassoon and recorder. I used to play bassoon in orchestras at school and university. I still play the piano for recreation, and go to lots of classical music concerts."

To conclude the interview, I asked whether Dr Hodgson had always planned a career in mathematics. His reply was simple yet profound:

> "I had other interests — physics and meteorology — but maths was the most interesting."

— James Saunderson

The RSA Challenge

Observe that

$$\begin{gathered}
398075086424064937397125500550386491199064362 \\
34252670840638518957594638895726176858 3317 \\
\times \\
4727721461074353025362230719730482246329146 9 \\
53020971164598521711305207112563635903975 27 \\
= \\
1881988129206079638386972394616504398071635 6 \\
3379417382700763356422988859715234665485319 0 \\
6060650474304531738801130339671619969232120 \\
5734031879550656996221305168759307650257059
\end{gathered}$$

“Pooh-pooh”, I hear you say. “I learnt how to do long multiplication in year two.” Yet Jens Franke, of the German Federal Agency for Information Technology Security, and his cohort of codebreakers won \$10 000 for exactly that observation, which they made on December 3, 2003.

The number above is known as ‘RSA–576’ (so called because it has 576 digits when written in binary), and is one of a number of large integers that RSA Laboratories have published, with large cash prizes for anyone who can factorize one of them. If you think you would like a slice of this mathematical pie, and an international renown amongst mathematicians to boot, there are prizes of up to \$200 000 available for factorizations of the numbers at

`http://www.rsasecurity.com/rsalabs/challenges/factoring/numbers.html`

But beware: the largest (and most valuable) number on the list, RSA–2048, has 617 decimal digits! The problem of factorizing large numbers is notoriously difficult. Of course, given a large number, you can simply try dividing it by all the numbers less than it until you find a divisor, but that takes forever (well, not literally). There are some clever ways that make the process faster, but it is nevertheless a prohibitively slow process. Jens Franke and his team, despite using high-powered computing equipment at German universities, still took a highly non-trivial amount of time.

Using some ingenuity, it is possible to make codes which are extremely difficult to break, based on this idea. RSA is one such code (RSA stands for Rivest, Shamir and Adleman, the inventors of the code). It is one of the most widely-used methods of encryption in the world. If a message is encoded using RSA, decoding it without knowledge of the 'key' requires the factorization of a large composite number into two large primes (see the next section for more detail on how RSA works). So if we choose two humongously large primes for our code, current techniques of factorization will take a few squillion years before they are able to break the code, so our correspondence is effectively safe.

What makes the people of RSA security a bit edgy, however, is that no one has *proven* that there is no quick way of factorizing large numbers. "What if," they ask themselves in querulous voices, "What if some unknown genius discovers a new, incredible method of factorization that makes our product obsolete?" This is the reason for the RSA challenge. By offering prizes for the factorizations of large numbers, RSA should be able to determine roughly how big their primes need to be to make factorization effectively impossible.

This was shown to be a very wise move by the case of RSA–129. The inventors of RSA published this number, and encoded a message using the RSA method. They offered $100 to anyone who could decode the message. One of the inventors made the rather extravagant claim that this code would take forty quadrillion years to break, which made him look a right fool when it was broken in 1994, and he looked even more foolish when it was revealed that the encoded message was "The magic words are squeamish ossifrage"[1].

So, if you think you are up for a challenge, give some of the RSA numbers a try. But if you **do** discover a new and effective way of factorizing large numbers, you could probably make more money by keeping your discovery secret and working for the NSA than by cleaning up on the RSA challenge numbers. Keep that in mind.

The Theory Behind RSA

To put RSA into practice, I choose two large primes, p and q, and I make their product public. I also choose two other integers, d and e, so that

$$de \equiv 1 \mod (p-1)(q-1)$$

I also make d public, but I keep e, p and q secret. If you want to send me a message, you turn it into a number, M (this is not too difficult to do - you

[1] An ossifrage, it seems, is a rare European species of predatory vulture.

can use the ASCII values of letters). Now you send me the 'encrypted' number $M^d \pmod{pq}$. When I get it, I work out $(M^d)^e \pmod{pq}$. You can prove that this will be the original message, that is, $M^{de} \equiv M \mod pq$. This is because $(p-1)(q-1) = \phi(pq)$, where $\phi(n)$ is the number of numbers less than n which are relatively prime to n. Euler proved that, if $\gcd(a, n) = 1$, then

$$a^{\phi(n)} \equiv 1 \mod n$$

so

$$M^{de} \equiv M^{k\phi(pq)+1} \equiv M \mod pq$$

(by the way we defined e and d) and so I will obtain the original message from your encoded message. So, to discover e and hence decode the message, a codebreaker must know $(p-1)(q-1)$, which is equivalent to factorizing pq. If we choose p and q to be fantastically large, the codebreaker doesn't have a prayer, and we're safe.

So, for example, I might choose $p = 29$, $q = 67$, $d = 65$, $e = 1649$. Note that

$$65 \times 1649 \equiv 1 \mod (28 \times 66)$$

So I make public the numbers 65 and 1943 (which is 29×67). Now suppose you want to send the message 'NO'. 'N' is the 14th, and 'O' is the 15th letter of the alphabet, so you make your message $M = 1415$. Then you encode your message:

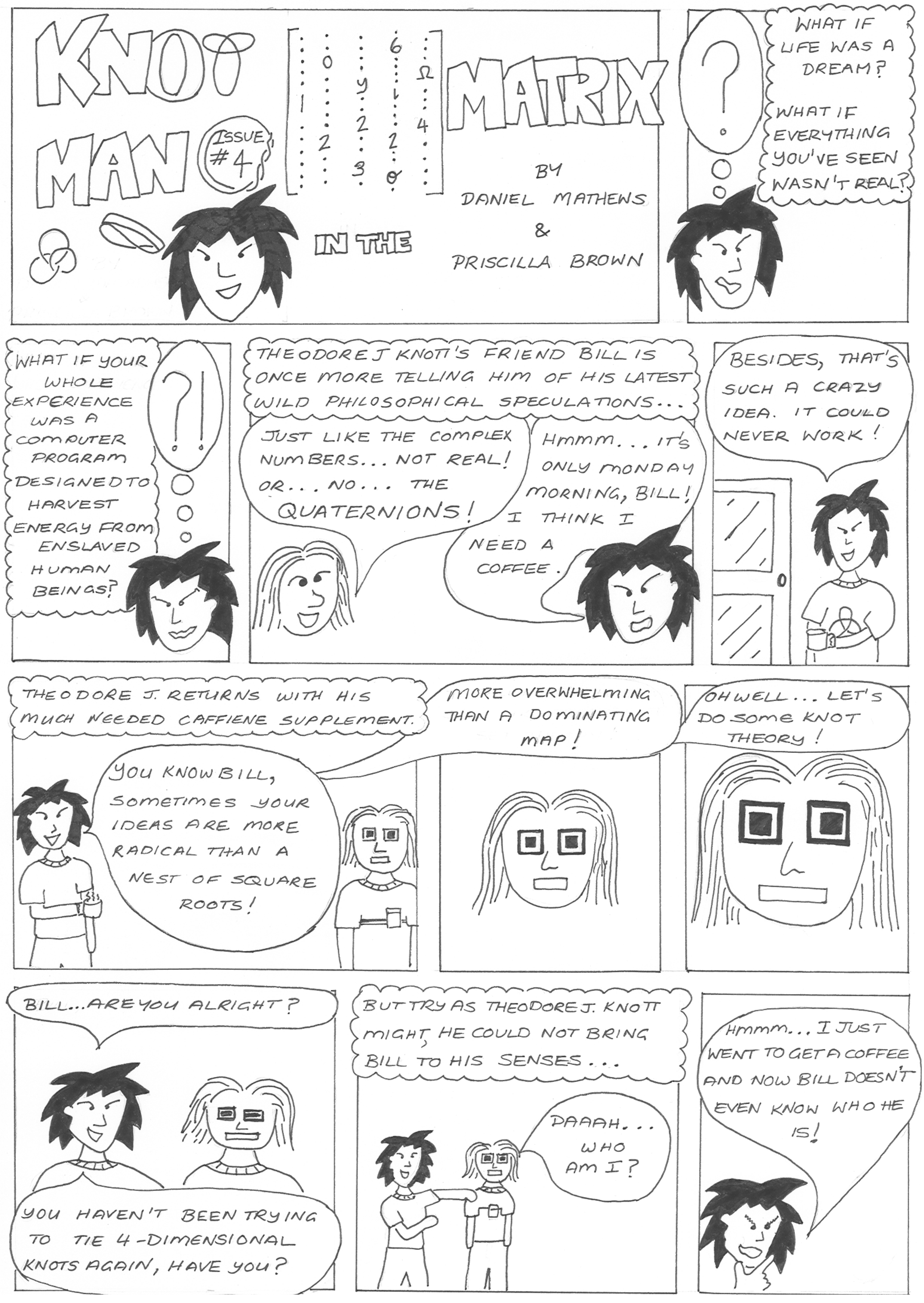
$$M^d \equiv 1415^{65} \equiv 645 \mod 1943$$

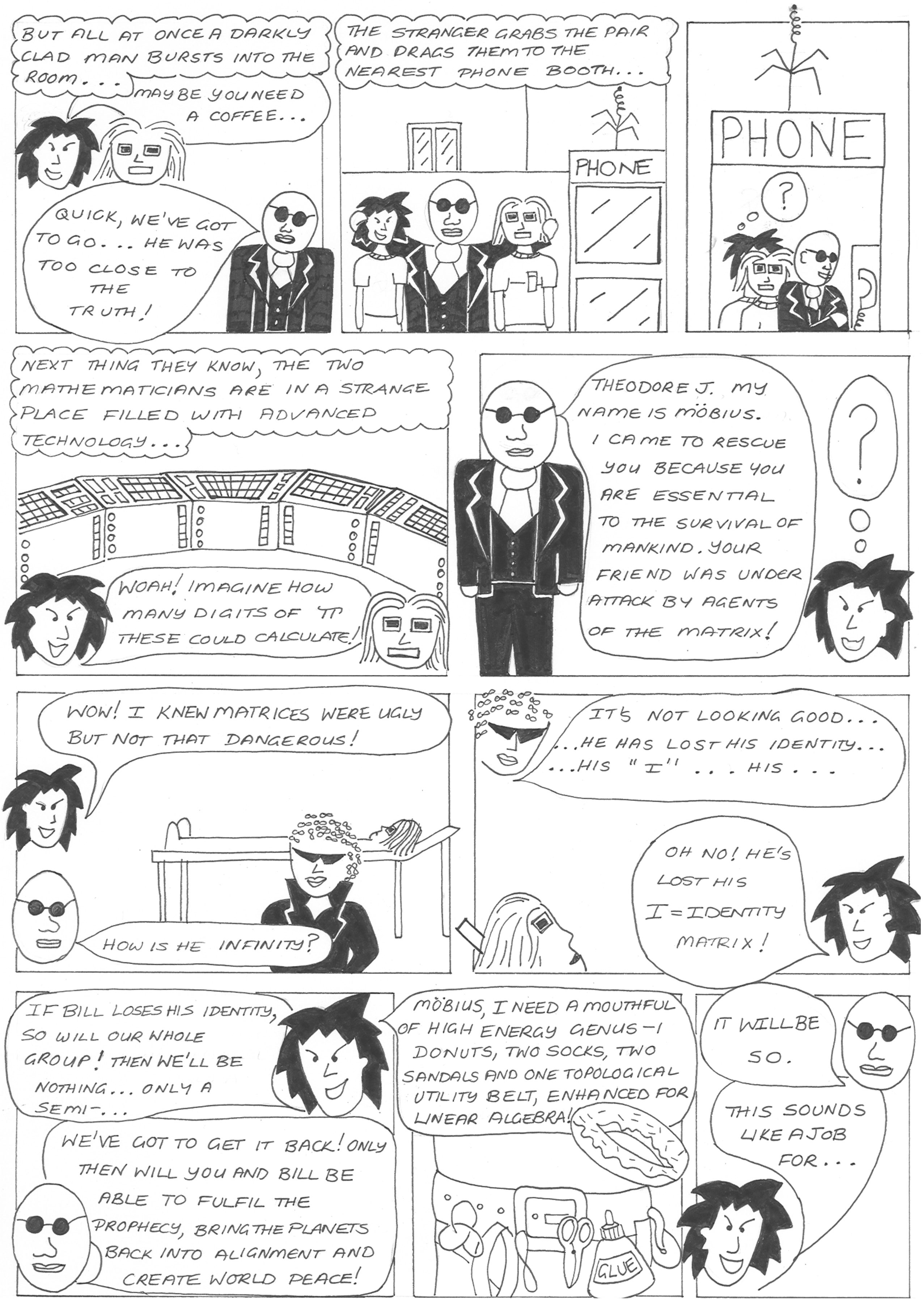
If I now want to decode it, I calculate

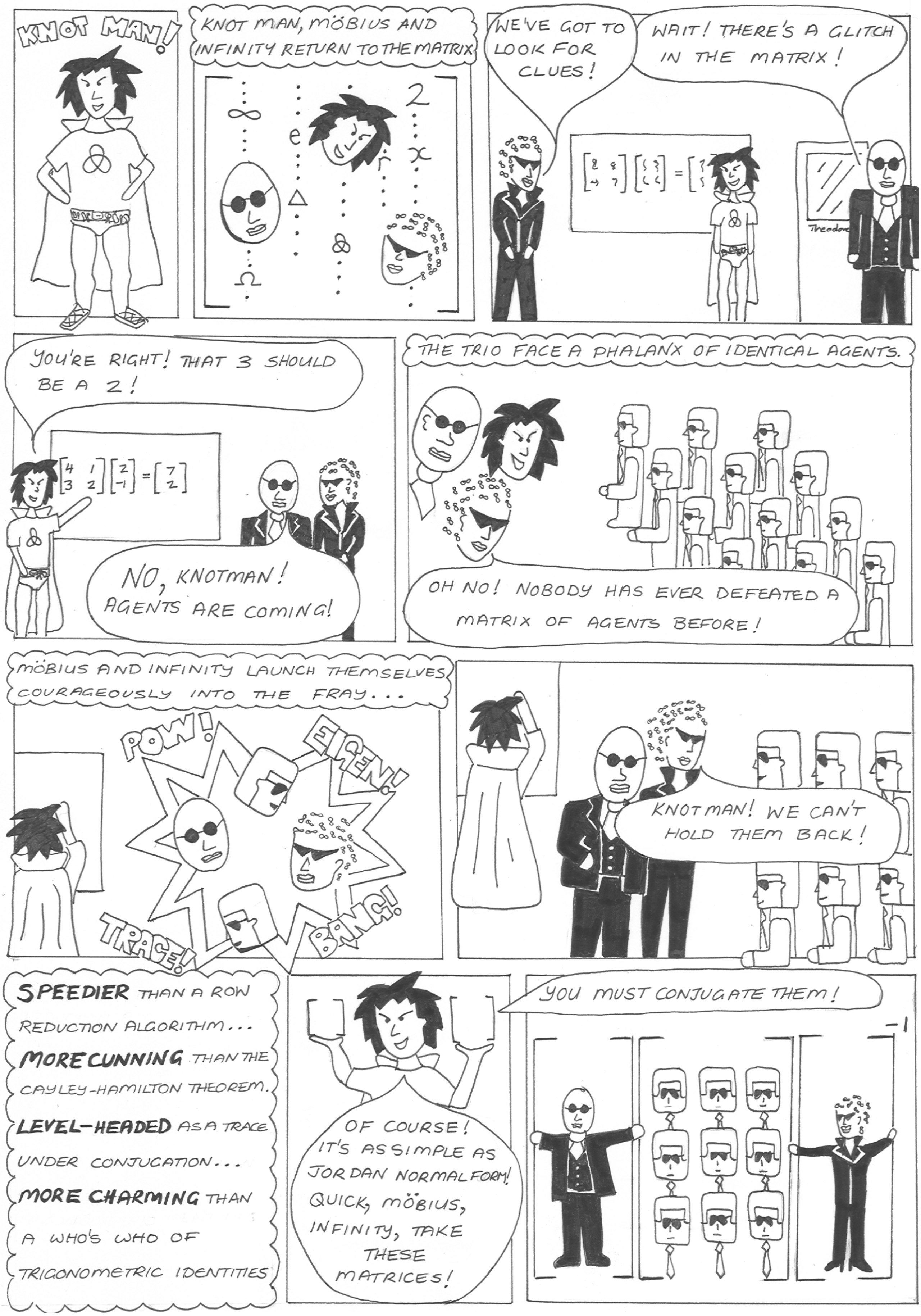
$$645^{1649} \equiv 1415 \mod 1943$$

So I recover your message. If someone wanted to decode your message, they would be forced to factorize 1943. You may worry that someone could guess your message, and check if they were correct by encoding their guess to see if it gave the same value as your encoded message. In practice, random digits are put at the end of the message before it is encoded, to prevent this sort of attack.

— Nick Sheridan


KNOT MAN
ISSUE #4
IN THE
MATRIX
BY
DANIEL MATHEWS
&
PRISCILLA BROWN
WHAT IF LIFE WAS A DREAM?
WHAT IF EVERYTHING YOU'VE SEEN WASN'T REAL?
WHAT IF YOUR WHOLE EXPERIENCE WAS A COMPUTER PROGRAM DESIGNED TO HARVEST ENERGY FROM ENSLAVED HUMAN BEINGS?
THEODORE J KNOTT'S FRIEND BILL IS ONCE MORE TELLING HIM OF HIS LATEST WILD PHILOSOPHICAL SPECULATIONS...
JUST LIKE THE COMPLEX NUMBERS... NOT REAL! OR... NO... THE QUATERNIONS!
HMMM... IT'S ONLY MONDAY MORNING, BILL! I THINK I NEED A COFFEE.
BESIDES, THAT'S SUCH A CRAZY IDEA. IT COULD NEVER WORK!
THEODORE J. RETURNS WITH HIS MUCH NEEDED CAFFIENE SUPPLEMENT.
YOU KNOW BILL, SOMETIMES YOUR IDEAS ARE MORE RADICAL THAN A NEST OF SQUARE ROOTS!
MORE OVERWHELMING THAN A DOMINATING MAP!
OH WELL... LET'S DO SOME KNOT THEORY!
BILL... ARE YOU ALRIGHT?
YOU HAVEN'T BEEN TRYING TO TIE 4-DIMENSIONAL KNOTS AGAIN, HAVE YOU?
BUT TRY AS THEODORE J. KNOTT MIGHT, HE COULD NOT BRING BILL TO HIS SENSES...
DAAAH... WHO AM I?
HMMM... I JUST WENT TO GET A COFFEE AND NOW BILL DOESN'T EVEN KNOW WHO HE IS!


BUT ALL AT ONCE A DARKLY CLAD MAN BURSTS INTO THE ROOM...
MAYBE YOU NEED A COFFEE...
QUICK, WE'VE GOT TO GO... HE WAS TOO CLOSE TO THE TRUTH!
THE STRANGER GRABS THE PAIR AND DRAGS THEM TO THE NEAREST PHONE BOOTH...
PHONE
PHONE
?
NEXT THING THEY KNOW, THE TWO MATHEMATICIANS ARE IN A STRANGE PLACE FILLED WITH ADVANCED TECHNOLOGY...
WOAH! IMAGINE HOW MANY DIGITS OF π THESE COULD CALCULATE!
THEODORE J. MY NAME IS MÖBIUS. I CAME TO RESCUE YOU BECAUSE YOU ARE ESSENTIAL TO THE SURVIVAL OF MANKIND. YOUR FRIEND WAS UNDER ATTACK BY AGENTS OF THE MATRIX!
?
WOW! I KNEW MATRICES WERE UGLY BUT NOT THAT DANGEROUS!
HOW IS HE INFINITY?
IT'S NOT LOOKING GOOD... ...HE HAS LOST HIS IDENTITY... ...HIS "I" ... HIS ...
OH NO! HE'S LOST HIS I = IDENTITY MATRIX!
IF BILL LOSES HIS IDENTITY, SO WILL OUR WHOLE GROUP! THEN WE'LL BE NOTHING... ONLY A SEMI-...
WE'VE GOT TO GET IT BACK! ONLY THEN WILL YOU AND BILL BE ABLE TO FULFIL THE PROPHECY, BRING THE PLANETS BACK INTO ALIGNMENT AND CREATE WORLD PEACE!
MÖBIUS, I NEED A MOUTHFUL OF HIGH ENERGY GENUS-1 DONUTS, TWO SOCKS, TWO SANDALS AND ONE TOPOLOGICAL UTILITY BELT, ENHANCED FOR LINEAR ALGEBRA!
GLUE
IT WILL BE SO.
THIS SOUNDS LIKE A JOB FOR...


KNOT MAN!
KNOT MAN, MÖBIUS AND INFINITY RETURN TO THE MATRIX
WE'VE GOT TO LOOK FOR CLUES!
WAIT! THERE'S A GLITCH IN THE MATRIX!
Theodore
YOU'RE RIGHT! THAT 3 SHOULD BE A 2!
NO, KNOTMAN! AGENTS ARE COMING!
THE TRIO FACE A PHALANX OF IDENTICAL AGENTS.
OH NO! NOBODY HAS EVER DEFEATED A MATRIX OF AGENTS BEFORE!
MÖBIUS AND INFINITY LAUNCH THEMSELVES COURAGEOUSLY INTO THE FRAY...
POW!
EIGEN!
TRACE!
BANG!
KNOTMAN! WE CAN'T HOLD THEM BACK!
SPEEDIER THAN A ROW REDUCTION ALGORITHM...
MORE CUNNING THAN THE CAYLEY-HAMILTON THEOREM.
LEVEL-HEADED AS A TRACE UNDER CONJUGATION...
MORE CHARMING THAN A WHO'S WHO OF TRIGONOMETRIC IDENTITIES
OF COURSE! IT'S AS SIMPLE AS JORDAN NORMAL FORM! QUICK, MÖBIUS, INFINITY, TAKE THESE MATRICES!
YOU MUST CONJUGATE THEM!
-1


SURELY ENOUGH, THE AGENTS WERE DIAGNOLIZED AND DISPERSED ALONG VARIOUS EIGEN VECTORS!
GOOD WORK, KNOT MAN! NOW LET'S FIND BILL'S IDENTITY MATRIX!
THROUGH A DOOR, AND THEY FIND THEMSELVES IN A CHAMBER, CONFRONTED BY A RATHER POMPOUS CHARACTER.
THE ARCHITECT!
REALITY BLAH FATE EQUATION BLAH BLAH FREE WILL BLAH BLAH.
OH NO! THIS GUY'S PHILOSOPHICAL MUMBO JUMBO IS WORSE THAN AN ARTS TUTE!
BUT THEN, PREVIOUS VERSIONS OF THE MATRIX FAILED. WHY?
KNOT MAN HAS A SUITABLE REPLY TO THIS DUBIOUS QUESTION.
BUT IN SPECIAL MATRICES, THE DETERMINANT IS ALWAYS THE ONE!
!
WITH THE ARCHITECT DAZED AND CONFUSED BY HIS OWN NONSENSE, KNOT MAN SPRINTS TO THE DOOR... TO WHATEVER THE ARCHITECT IS GUARDING...
WHO ARE YOU?
I AM THE ONE.
A MULTIPLICATIVE IDENTITY?
THE ONE.
YOU LOOK LIKE KEANU REEVES TO ME...
LOOK! WE WON!
THE ONE!
WHO WON?
THE ONE.
ONE WON?!
MR THE ONE, CAN YOU PUT THE 1's BACK IN BILL'S IDENTITY MATRIX?
IT IS DONE.
PARTY ON DUDE!
?!
BILL'S IDENTITY IS RETURNED...
THANKS A KNOT!
TIME FOR US TO TAKE A COORDINATE CHART HOME!
... AND BACK TO REALITY
HMMM... I JUST HAD THE STRANGEST DREAM...
$\begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix}\begin{bmatrix} 2 \\ -1 \end{bmatrix} = \begin{bmatrix} 7 \\ 2 \end{bmatrix}$
Zzz
KNOT MAN! MASTER OF THE MATRIX!
1
$\lambda_1 \; \lambda_2 \; \lambda_3 \ldots \lambda_n$
QED

Mathematical Poetry Competition!

Paradox is now accepting entries for its second ever Mathematical Poetry Competition. So if you have a desire to express the inner mathematician in you through verse, then please send your creations to paradox@ms.unimelb.edu.au. The best entries will be printed in the next issue and winners will be in line to receive a free subscription to Paradox for 2004! The following is a collection of mathematical poems to inspire you.

A mathematician confided
That the Möbius band is one-sided
And you'll get quite a laugh
If you cut one in half
'Cause it stays in one piece when divided.

A challenge for many long ages
Had baffled the savants and sages.
Yet at last came the light:
Seems old Fermat was right —
To the margin add 200 pages.

π goes on and on and on…
And e is just as cursed.
I wonder: Which is larger
When their digits are reversed?

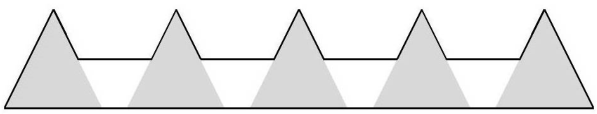
A mathematician named Klein
Thought the Möbius band was divine
Said he: If you glue
The edges of two
You'll get a weird bottle like mine.

A graduate student from Trinity
Computed the cube of infinity;
But it gave him the fidgets
To write down those digits,
So he dropped maths and took up divinity.

Art Gallery Theorems

Imagine that you are the owner of several art galleries and that you are in the process of hiring people to guard one of them. Unfortunately, with so many art galleries in your possession, you have forgotten the exact shape of this particular one. In fact, all you can remember is that the art gallery has the shape of a polygon with n sides. Of course, guards have the capacity to turn around a full 360° and can see everything in their line of sight, but being terribly unfit, are unwilling to move. So my question to you is the following... what is the minimum number of guards that you need to be sure that they can watch over the entire art gallery?

This question was first posed in 1973 by Victor Klee when asked by fellow mathematician Vašek Chvátal for an interesting problem. Consider the comb-shaped art gallery below which has fifteen sides. It is clear that at least one guard is required to stand in each of the shaded areas in order to keep an eye on each of the "prongs" of the comb. Thus, at least five guards are needed to watch over the entire art gallery, and you can check that five are actually sufficient. In fact, it is not too difficult to see that you can form a k-pronged comb-shaped art gallery which has $3k$ sides and requires k guards. Furthermore, by chipping off a corner or two from a k-pronged comb-shaped art gallery, it is clear that there exist art galleries which have $3k+1$ or $3k+2$ sides which require k guards. In short, we have shown there are art galleries with n sides that need $\lfloor n/3 \rfloor$ guards[1].



So you will need to hire at least $\lfloor n/3 \rfloor$ to guard your art gallery, but is it possible that you might need even more? The following theorem states that you don't, which means that the comb-shaped art gallery actually gives a worst case scenario.

Art Gallery Theorem: Only $\lfloor \frac{n}{3} \rfloor$ guards or fewer are required to watch over an art gallery with n sides.

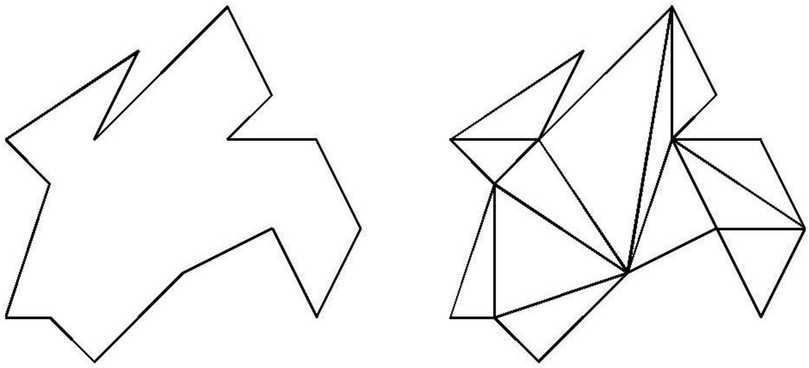
[1] Here, we use the notation $\lfloor x \rfloor$ to denote the largest integer less than or equal to x.

A Not-Too-Scary Proof of the Art Gallery Theorem

In 1978, a "proof from the book"[2] was found by Steve Fisk, and this is the one which we will present. There are three main steps in his line of reasoning.

- *You can always triangulate a polygon.*
  To triangulate a polygon is to divide it up into triangular regions by joining up pairs of vertices. The fact that this is true follows from the following[3]

  > Useful Lemma: In any polygon with more than three sides, there exists a diagonal joining two of the vertices which lies completely inside the polygon.

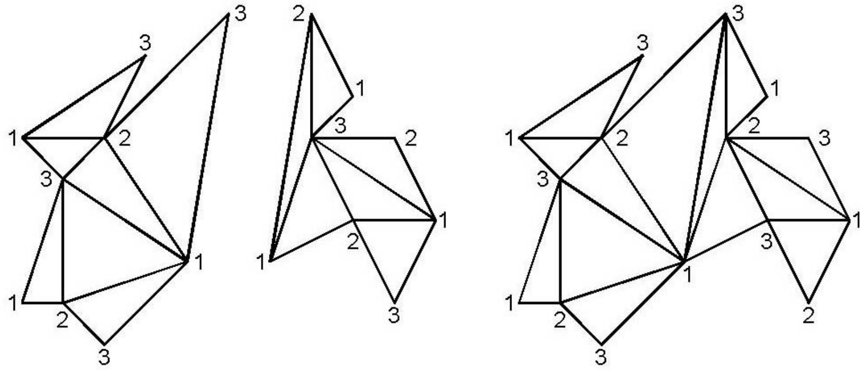


- *There is a nice colouring of every triangulation of a polygon which uses only three colours.*
  A nice colouring is a way to assign a colour (or, due to the monochromatic nature of Paradox, a number) to each vertex of the triangulation so that every triangle has corners with three different colours. Given only three colours, this is an easy task if the polygon is a triangle, so let us consider what happens when there are more than three sides. But then by the useful lemma which we stated above, there exists a diagonal joining two of the vertices which lies completely inside the polygon. Suppose that we use this diagonal to split our art gallery into two separate ones. Notice now that if we can nicely colour the two smaller art galleries, then they

[2] The renowned twentieth century mathematician Paul Erdős liked to talk about "The Book", in which God maintains the perfect proofs for mathematical theorems.

[3] For those unaware, a lemma is not actually half of a dilemma, but the fancy name that mathematicians give to a handy little theorem which they are using to prove a bigger theorem.

can be glued together, after relabelling the colours in one of the pieces, to give a nice colouring of the original art gallery. But can we nicely colour these two smaller art galleries with three colours? Of course we can. . . just use the same trick to split them up into smaller and smaller pieces until we are left merely with triangles, which can obviously be nicely coloured!



- *Now place your guards at the vertices which have the minority colour.* Suppose that the colour which occurs the least number of times is red, for example, and that there are actually k red vertices. Since there are n vertices altogether and only three colours, that tells us that $k \leq n/3$ and since k is an integer, we have $k \leq \lfloor n/3 \rfloor$. But what happens when we place k guards at these red vertices? Well, by the properties of a nice colouring, every triangle in the triangulation contains a red vertex and a guard standing at this vertex can obviously watch over every part of that triangle. So every triangle in the triangulation is being watched over by at least one guard and hence, every point in the art gallery is being watched over by at least one guard.

More Art Gallery Theorems and Unsolved Problems

Imagine now that you have suddenly remembered that your art gallery isn't just any old random polygon with n sides, but actually satisfies the condition that any two walls which meet do so at right angles. This is known as an orthogonal art gallery for obvious reasons and we have the following result.

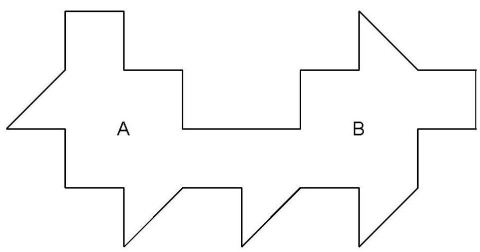
Orthogonal Art Gallery Theorem: Only $\lfloor \frac{n}{4} \rfloor$ guards or fewer are required to watch over an orthogonal art gallery with n sides.

Or suppose that you have enough money to hire fit guards who don't just stand still but patrol along a particular wall of the art gallery. How many of these "wall guards" are required to watch over the art gallery? Interestingly enough, the answer is unknown, but the following is believed to be true.

> Art Gallery Conjecture for Wall Guards: Only $\lfloor \frac{n}{4} \rfloor$ wall guards or fewer are required to watch over an art gallery with n sides, except for a few small special cases.

There are numerous other unsolved problems, such as considering art galleries with "holes" or the three dimensional analogue of the art gallery theorem. However, we will finish with an illuminating problem, which was brought to the attention of mathematicians in 1969 by Victor Klee, the very same person who brought you the original art gallery problem.

Imagine that you are standing in a room in the shape of a polygon and that each wall is a mirror. If you strike a match, is it always possible to illuminate the whole room? We will assume that light hitting a corner of the room is not reflected at all. This question was answered in 1995 by George Tokarsky, using the following example. He showed that if you are standing at point A, then you can not illuminate the whole room — in fact, you can not illuminate the point B. This example uses a polygon with 26 sides, but can you find one which is smaller?



It turns out that even though you cannot illuminate the whole room while standing at the point A, you certainly can do so by moving to another point of the room. We will leave the reader with the following unsolved problem.

> Is it true that in a polygonal room whose walls are mirrors, there is always a point from which we can illuminate the whole room?

— Norman Do

Maths Jokes and Quotes

$$\lim_{x \to 8} \frac{1}{x-8} = \infty$$

$$\Rightarrow \lim_{x \to 5} \frac{1}{x-5} = 5$$

Anyone who cannot cope with mathematics is not fully human. At best he is a tolerable subhuman who has learned to wear shoes, bathe and not make messes in the house.

Lazarus Long, "Time Enough for Love"

What is the origin of the urge, the fascination that drives physicists, mathematicians, and presumably other scientists as well? Psychoanalysis suggests that it is sexual curiosity. You start by asking where little babies come from, one thing leads to another, and you find yourself preparing nitroglycerine or solving differential equations. This explanation is somewhat irritating, and therefore probably basically correct.

David Ruelle, "Chance and Chaos"

A seven-year-old of my acquaintance claimed that the last number of all was 23,000. "What about 23,000 and one?" she was asked. After a pause: "Well, I was close."

Robert Kaplan, "The Nothing That Is"

By keenly confronting the enigmas that surround us, and by considering and analyzing the observations I had made, I ended up in the domain of mathematics.Although I am absolutely without training in the exact sciences, I often seem to have more in common with mathematicians than with my fellow artists.

M. C. Escher

I've dealt with numbers all my life, of course, and after a while you begin to feel that each number has a personality of its own. A twelve is very different from a thirteen, for example. Twelve is upright, conscientious, intelligent, whereas thirteen is a loner, a shady character who won't think twice about breaking the law to get what he wants. Eleven is tough, an outdoorsman who likes tramping through woods and scaling mountains; ten is rather simpleminded, a bland figure who always does what he's told; nine is deep and mystical, a Buddha of contemplation.

Paul Auster, "The Music of Chance"

The combination of the discoveries of Einstein and Pythagoras:

$$E = mc^2 = m(a^2 + b^2)$$

Sylvester was once approached by one of his research students who proposed to use a certain result in his research. Sylvester objected that the claimed theorem could not possibly be true, at which point the student tactfully explained to him that he, Professor Sylvester, had proved it himself, many years previously.

A. R. Luria, "The Mind of a Mnemonist"

Thanks

The Paradox team would like to thank Daniel Mathews, James Saunderson, Julian Assange, Nicholas Sheridan, Priscilla Brown and Sally Zhao for making contributions to this issue. Thanks must also go to Andrew Kwok, Denise Lin and Stephen Farrar for their help with editing and layout. We would also like to thank Punya Mishra for allowing us to use his artwork for the front cover and Craig Hodgson for taking time out of his busy schedule to be interviewed.

Paradox Problems

The following are some maths problems for which prize money is offered. The person who submits the best (clearest and most elegant) solution to each problem will be awarded the sum of money indicated beside the problem number. Solutions may be emailed to

`paradox@ms.unimelb.edu.au`

or you can drop a hard copy of your solution into the MUMS pigeonhole near the Maths and Stats Office in the Richard Berry Building.

1. *Rearranging digits* ($5)
   Can you find an integer beginning with the digit 1, such that when the digit 1 is moved to the other end you get three times the number you started with? Can you find an integer with the same property but beginning with the digit 2?

2. *Coins in a row* ($5)
   On a table is a row of fifty coins, of various denominations. Alice picks a coin from one of the ends and puts it in her pocket; then Bob chooses a coin from one of the remaining ends and the alternation continues until Bob pockets the last coin. Prove that Alice can play so as to guarantee that she will end up with at least as much money as Bob.

3. *Spot the pattern* ($5)
   The squares of an infinite chessboard are numbered as illustrated. The number 0 is placed in the upper left-hand corner; each remaining square is numbered with the smallest nonnegative integer that does not already appear to the left of it in the same row or above it in the same column. Which number will appear in the 2004th row and 1729th column?

0	1	2	3	4	5	
1	0	3	2	5	4	
2	3	0	1	6	7	
3	2	1	0	7	6	
4	5	6	7	0	1	
5	4	7	6	1	0	

4. *Dominoes* (\$5)
A complete domino set (which consists of the 28 dominoes 0-0, 0-1, 0-2, ..., 6-6) has been placed in the following diagram. However, all of the edges of the dominoes have been removed and there are blank spaces to be filled with each of the numbers 0, 1, 2, 3, 4, 5, 6. Fill these seven spaces and determine where the edges of the dominoes must be. Your solution must obey the extra condition that the adjacent 4 and 0 in the first row cannot be joined to form the domino 0-4.

3	4	0	1	0	6	4	3
2	6	6	0	6	1	0	2
1	6		5	2	6	5	
	1	6	1	2	3	4	
5	3	5	2		4	0	2
1	0		5	5	5	2	
4	1	0	3	3	4	4	3

5. Mathematics and Statistics courses (\$5)
This semester, the Mathematics and Statistics Department is offering its students Complex Analysis and four other courses. Each class is offered on a different day from Monday to Friday, and each is taught by a different lecturer. From the data given below, can you determine which course is given on which day and the full name (one last name is Chan) of the lecturer?

   (a) Peter and Borovkov both work full-time and teach at university part-time.
   (b) Derek's class is later in the week than Taylor's, but earlier in the week than Operations Research.
   (c) The Metric Spaces course is offered Thursday.
   (d) Kostya's class isn't on Monday.
   (e) Jerry, Rubinstein, and the Metric Spaces lecturer all hold PhD's in mathematics.
   (f) Koliha teaches the day before Peter, who teaches the day before Jerry.
   (g) Derek's course isn't Probability.
   (h) Koliha, who isn't Hyam, teaches a class held earlier in the week than Number Theory.

Melbourne University
Mathematics and Statistics Society

Upcoming Events:

Event:	*Date:*
• **Seminar**	**Friday 23 April**
• **BBQ**	**Friday 30 April**
• **A.G.M.**	**Friday 7 May**
• **Trivia Night**	**T.B.A.**

For more information:

- keep an eye out for posters in the Richard Berry Building
- subscribe to our mailing list at:

  `http://www.ms.unimelb.edu.au/~mums/mlist`