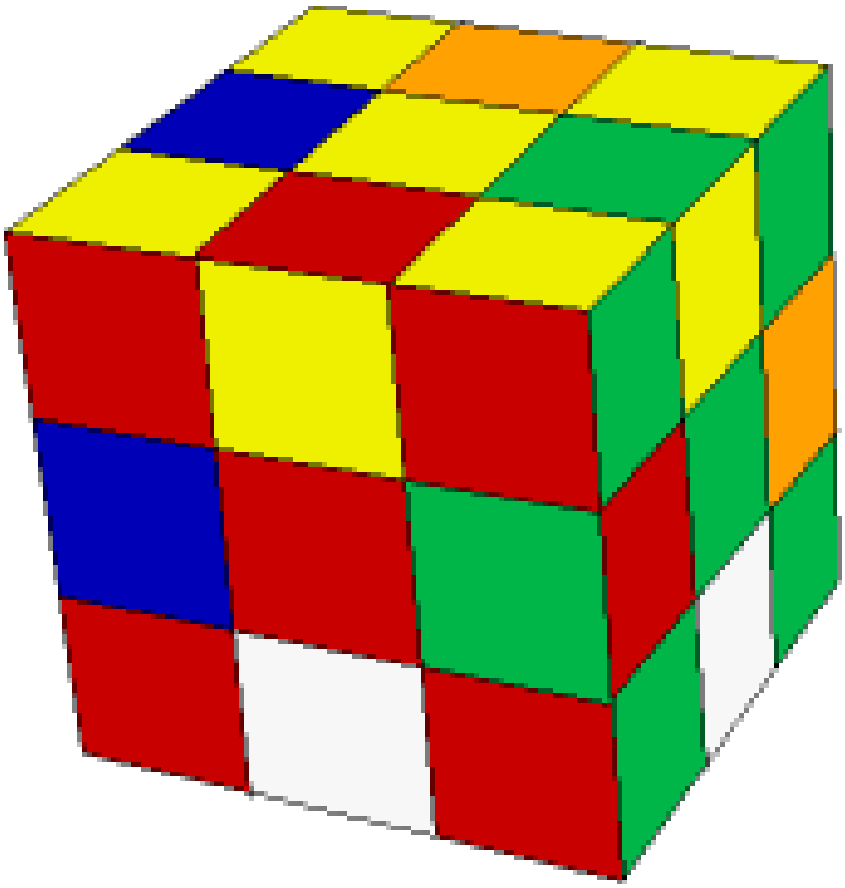
Paradox

Issue 1, 2011

THE MAGAZINE OF THE MELBOURNE UNIVERSITY MATHEMATICS AND STATISTICS SOCIETY



MUMS

PRESIDENT:	Sam Chow cme_csamc@hotmail.com
VICE-PRESIDENT:	Muhammad Adib Surani m.surani@ugrad.unimelb.edu.au
TREASURER:	Julia Wang julia.r.wang@gmail.com
SECRETARY:	Mark Kowarsky mark@kowarsky.id.au
EDUCATION OFFICER:	Richard Hughes mobyseven@gmail.com
PUBLICITY OFFICER:	Brendan Duong b.duong@ugrad.unimelb.edu.au
EDITOR OF Paradox:	Stephen Muirhead s_muirhead22@hotmail.com
UNDERGRAD REP:	Mel Chen m.chen11@ugrad.unimelb.edu.au
UNDERGRAD REP:	Narthana Epa narthana.epa@gmail.com
UNDERGRAD REP:	Ahmad Issa a.issa2@ugrad.unimelb.edu.au
UNDERGRAD REP:	Dana Ma iwantakudamon@hotmail.com
UNDERGRAD REP:	David Schlesinger d.schlesinger@ugrad.unimelb.edu.au
UNDERGRAD REP:	Trithang Tran t.tran17@ugrad.unimelb.edu.au
POSTGRADUATE REP:	Jeff Bailes j.bailes@pgrad.unimelb.edu.au
POSTGRADUATE REP:	Yi Huang y.huang16@pgrad.unimelb.edu.au

WEB PAGE:	http://mums.org.au
MUMS EMAIL:	mums@ms.unimelb.edu.au
PHONE:	(03) 8344 4021

In this edition of Paradox

Regulars

Special Features

Articles

EDITOR: Stephen Muirhead
SUB-EDITORS: Mel Chen, Richard Hughes, Kristijan Jovanoski, Jiaying Zhang
WEB PAGE: www.ms.unimelb.edu.au/~paradox
E-MAIL: paradox@ms.unimelb.edu.au
PRINTED: 22 February, 2011
COVER: A Rubik's Cube in the 'superflip' position (see page 16 for details)

Words from the Editor

Six months is a long time in the world of maths-focused student magazines. Although Paradox itself may have been quiet, there has certainly been upheaval for two of the protagonists from the last edition (Issue 2, 2010 – check the MUMS website for full archives of Paradox).

First, Julian Assange has morphed from little-known internet activist to arguably the world's most notorious man, earning praise and reproach in equal measure for his website Wikileaks's massive release of confidential US government cables (you can read about Julian's involvement with MUMS in the previous edition). So high has his influence risen, that his mere mention that Wikileaks possessed documents relating to a large American bank was enough to cause Bank of America's share price to plummet 3.2 percent in a day.[1] Narrowly beaten out for TIME's 'Person of the year' by Mark Zuckerburg, Julian is also on the point of publishing his much-awaited biography.[2] Finally, and most seriously, there is the matter of his arrest and detention in London on questionable rape allegations originating from Sweden. Julian's extradition hearing is currently ongoing; Paradox wishes him all the best.

Second, on a different note, Paul the Octopus died a quiet death in his aquarium in Germany in October, with a shrine put up to honour his oracular prowess demonstrated most emphatically at the 2010 World Cup (read about the maths behind Paul's predictions in the last edition). A successor to Paul has already been appointed by his aquarium – look out for Paul II's predictions at the 2014 European Championship.

Meanwhile, in the pages of this edition you can read about another MUMS's alumnus, John Dethridge, and his involvement in the search for the Rubik's cube 'God number'. Elsewhere, you can sample films from the 'maths thriller' genre, tackle the *Kryptos* puzzle, explore the lives of famous mathematicians, delve into the unsolved, million-dollar *p v np* problem, and read about the link between maths and Charles Darwin.

Finally, Paradox would like to reiterate that it is a student-run magazine, and relies on contributions from people like you! So, if you like what you read, feel free to get involved by dropping by the MUMS room or by emailing Paradox.

— Stephen Muirhead

[1] On November 30, 2010.

[2] It remains to be seen whether MUMS gets a mention.

Words from the President

Orientation, or perhaps reorientation: a very good place to start. A mass migration into our beloved base camp, the MUMS room, is keenly anticipated. If you're at all perplexed by my rather drawn out introduction, don't sweat it: you'll soon solve this puzzle.

Perhaps you'll solve a few more in this year's PuzzleHunt,[3] which is set for April 11-15. Find the hidden object to make $200, earn immortality in the next Paradox issue, and save the world from some highly original criminal masterminds. Get a team together early, for you're allowed up to ten people. The more the merrier, really!

Weekly seminars will recommence in week one, and we've booked Lowe Theatre for Fridays at 1pm. Refreshments will follow in the MUMS room.[4] These seminars are a chance to get a neat summary of some phenomenon that an academic has researched, thereby learning a little bit about all of the different areas of mathematics. It's also a good chance to meet like-minded people, for instance by using food as an excuse to step boldly into the MUMS room.

Also forthcoming are a games night or several (TBA), a trivia night (end of semester probably) and our AGM (towards the end of semester). For more information about our events, please go to `mums.org.au` and join our mailing list. In the meantime, you can check out our Facebook group, or drop by. A typical day in the MUMS room involves talking, going on the internet, and playing games. Yeah, we really like playing games. Also, there are MUMS T-shirts for sale.[5]

Finally, congratulations to T-boys (Trinity Grammar), who nudged out Curry in a Wok (Scotch College) to win the 2011 Schools Maths Olympics. The University Maths Olympics was won convincingly by Golden Staff (you young guns need to step up!). Thanks to MAV and ABS respectively for sponsoring these events.

— Sam Chow

[3] Google 'puzzle hunt' and use the left hand menu to navigate. Registration for this year's hunt should be open soon.

[4] Located opposite the main office in the Richard Berry building.

[5] $20, 100% cotton, interesting design!

Mathematical Miscellany

The following puzzles come from the film *Fermat's Room* (see page 7) – solutions are scattered throughout the edition (1,2: page 13; 3,4,5: page 19; 6,7: page 51):

1. A sweet seller receives three opaque boxes. One contains mint sweets, another aniseed sweets, and another a mix of the two. The boxes have labels which say 'mint', 'aniseed' or 'mixture', but the sweet seller is told that all the boxes are wrongly labelled. What is the minimum number of sweets the seller will have to take out to verify the contexts of the boxes?

2. Crack the following code:[6]

   0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1,1,0,0,0,1,1,1,1,1,1,1,
   1,1,1,1,0,0,1,1,1,1,1,1,1,1,1,1,1,0,0,1,1,0,0,0,1,0,0,0,1,1,0,0,1,1,
   0,0,0,1,0,0,0,1,1,0,0,1,1,1,1,1,1,0,1,1,1,1,1,0,0,1,1,1,1,0,0,0,1,1,1,
   1,0,0,0,1,1,1,1,1,1,1,1,1,0,0,0,0,0,1,0,1,0,1,0,1,0,0,0,0,0,0,1,1,0,
   1,0,1,1,0,0,0,0,0,0,1,1,1,1,1,1,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0

3. Inside a sealed room there is a light bulb. Outside the room there are three switches, only one of which lights the bulb. While the door is closed, you may press the switches as many times as you like. Can you determine, upon opening the door, which switch lights the bulb?

4. How can you time a period of nine minutes using two sand clocks, one of four minutes and one of seven?

5. A student asks his teacher: 'How old are your daughters?'. She replies: 'If you multiply their ages you get 36; if you add them, you get your house number'. 'I'm missing a detail', protests the student. The teacher replies: 'Yes; the eldest plays the piano.' How old are the daughters?

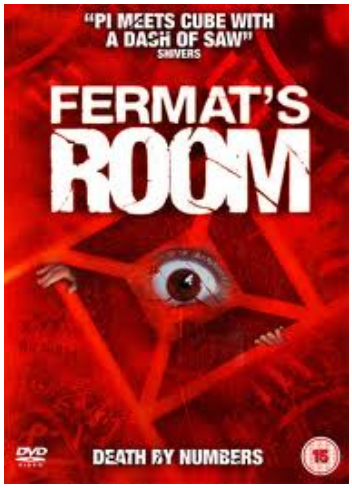
6. A stranger stands in a room with two doors. Only one door leads to freedom. Two jailers are in the room, one who tells only lies, and another who tells only truths; the stranger does not know who is who. The stranger may ask one question to one of the jailers. What can he ask so that he may determine which door leads to freedom?

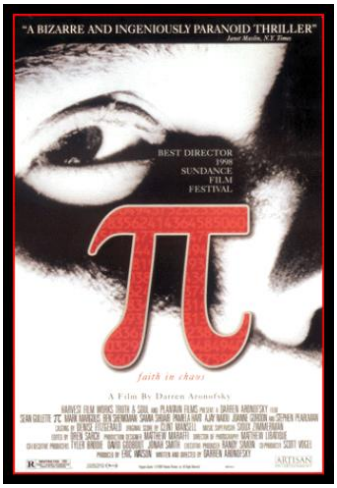
7. A mother is 21 years older than her son. In six years he will be five times younger than the mother. What is the father doing?

[6] This puzzle is, remarkably, near identical to Puzzle 2.1 from MUMS PuzzleHunt '05!

Of Murderers and Madmen: A review of *Fermat's Room* and *Pi*

What is it about mathematicians that make them such great fodder for horror films? Is it their ability to coldly calculate the perfect crime? Is it their single-minded dedication to their work, signalling a burgeoning madness? For this edition of Paradox, I braved two movies of the 'maths thriller' genre – *Fermat's Room* (originally, *La Habitatión de Fermat*), a 2007 Spanish film (the MUMS room has a copy for those interested in seeing it), and *Pi*, a 1998 film directed by cult favourite Darren Aronofsky – to find out exactly what it is about mathematicians that haunts the imaginations of ordinary citizens.





Fermat's Room (2007)

Four mathematicians – using the pseudonyms Pascal, Galois, Oliva[1] and Hilbert – are invited to a maths conference in a decrepit warehouse by a mysterious 'Fermat'. They explore the warehouse, and find themselves in a quaintly decorated conference room. The group soon finds themselves trapped inside, the walls slowly moving in, threatening to crush them unless they solve a series of puzzles.

Stylistically, *Fermat's Room* has a distinct Eurotrash feel. The plot doesn't entirely make sense, the soundtrack is inappropriately upbeat in otherwise ominous scenes, and there is a gratuitous amount of fast cars and sexual tension (for a horror movie about mathematicians, anyway).

[1] After Oliva Sabuco, a 16th century Spanish philosopher and doctor.

However, the puzzles in *Fermat's Room* redeem it of its cinematic shortcomings. Viewers have the pleasure of figuring out the core mysteries of the movie: who wants the mathematicians dead, and why? The audience is also invited to have a bit of fun by attempting to solve the puzzles given to the mathematicians while they are trapped inside the Room.[2] If you don't want to see the film, the puzzles are listed on page 6 of this edition, so you can try them at home; of course, you can make the experience all the more authentic by imagining that you too are in Fermat's Room, and must solve each puzzle within a minute, or otherwise face a gruesome death...

Finally, *Fermat's Room* asks: is it worthwhile for pure mathematicians to spend so much time and energy on something that has little practical application to our everyday lives? This question is posited through Pascal, the single applied mathematician in the group, who throughout the film is contrasted against his pure mathematician peers: while initially we ridicule him for spending his talents on designing duck-shaped popcorn machines, his knowledge about real world applications of mathematics – critically, how to use the furniture in the room to prevent the walls from enclosing further – are contrasted against the abilities of the pure mathematician Galois, who knows only to solve problems on a blackboard. At the very end, Pascal goes so far as to destroy the antagonist's proof of Goldbach's conjecture, suggesting that in the scheme of things, the study of pure mathematics is unimportant.

Pi (1998)

Pi was the breakthrough film by cult director Darren Aronofsky, also known for *Requiem for a Dream* (2000), *The Wrestler* (2008), and more recently, *Black Swan* (2010). Like Aronofsky's other films, *Pi* is a dark, psychological thriller, and explores the tension between the intellectual genius and mental afflictions of a reclusive number theorist, Max Cohen. Obsessed with his work, he believes that 'there are patterns everywhere in nature', and as long as he is able to decipher this pattern, he can understand how the universe works. '

With single-minded persistence, Cohen's research leads him to uncover this 'divine pattern', which turns out to be a sequence of 216 digits. However, as he begins to understand the sequence, outside commercial and religious interest groups push him to reveal his knowledge to them, and his paranoia and headaches intensify.

[2] One of which is, incidentally, identical to Puzzle 2.1 from PuzzleHunt '05 (see page 6)!

Unlike *Fermat's Room*, there are no puzzles and mathematical in-jokes. Instead, *Pi* examines the nature of obsession. In continuing with his intense research, Cohen sacrifices his mental and physical wellbeing, pushing forward despite experiencing severe shaking, nose bleeds and headaches. This is conveyed powerfully in the film by looking at the world from Cohen's point of view, so that the audience is placed through the same delusions and repetitious pill-taking, and haunted by the same searing noises. The black and white images go on to emphasise the madness and discord in Cohen's world. Thus, while he is finally 'enlightened' by the realisation of the 216-digit sequence, the audience is able to experience the terror of Cohen's madness and the overstepping of his mental and physical limitations.

Finally, *Pi* suggests that while mathematics has the potential to teach us precisely how the universe works, understanding only brings unhappiness. This message is carried throughout by Sol, Cohen's old mathematics mentor, who warns Cohen that 'there will be no order, only chaos', and persistently advises that Cohen takes a break. While the nature of Cohen's work is to show that there *is* order in nature, Cohen finally realises that the closer he gets to the 216-digit sequence, the more internal chaos he experiences. Only when Cohen self-lobotomises and lets go of both his ability and desire to understand does he find peace.

Conclusion

Popular culture has long sustained a stereotype for mathematicians: unkempt hair, antisocial and too engrossed in their higher study of mathematics to ever engage in the real world. Mathematical horror movies, as I have seen, take this concept one step further, and explore the more macabre extensions of this mathematician's personality. In *Fermat's Room*, the mathematician becomes a manipulative murderer, fixated on puzzles and twisted intellectual game play; and in *Pi*, he becomes the madman, so consumed by numbers and patterns and discovering the 'truth' that he descends into physical self-torture and insanity.

While one would hope that the film stereotypes of mathematicians are untrue, a visit to the MUMS room is enough to confirm that – in the company of tussle-haired, puzzle-hunting, bleary-eyed maths students – they not entirely unsubstantiated. Which is eerie. Don't take things any further folks.

— Jiaying Zhang

Letters and Numbers

There's something about these games that attracts maths students. It's not just the numbers, but the letters too! Why is it that we take an *mX* and immediately turn to the puzzles page to do the word jumbles? Why do we run a Puzzlehunt every year that's infested with wordplay which has nothing at all to do with maths? Do we all have an innate desire to case-bash?

Following on from the success of the equivalent French and British game shows, *Des chiffres et des lettres* and *Countdown*, Australia's very own *Letters and Numbers* pits people from all walks of life against one another in a nine round Blitzkrieg of word-spotting and quick arithmetic. I was fortunate enough to participate in Series One.[1]

After emailing an entry form, I was soon off to ABC studios in Elsternwick for an audition, along with about 20 others in the room. The main part of this was a test, which comprised letters rounds, numbers rounds, and two conundrums. I was accepted the next day, and chose some dates when I was free (I had to miss a day of Uni).

The rounds

Letters round

Nine letters are randomly assigned; one player designates 'vowel' or 'consonant' for each letter (at least three vowels and at least four consonants are

[1] MUMS members Muhammad Adib Surani and Michael Phillips also participated in Series One.

required). The players then make the longest word they can, using those letters (eg if there are two Rs displayed, then you can use at most two Rs in your word). The player with the longer word gets one point for each letter, whereas the other player gets nothing.

Numbers round
Six numbers are randomly assigned. 'Large' numbers are 25, 50, 75 and 100, while 'small' numbers are 1, 2...10. One player decides how many large numbers to have. A three-digit 'target' is also given. Players have to get as close to the target as possible using $+,-,\times,\div$ and parentheses. Arithmetic must be restricted to the integers (fractional intermediate totals are not permitted). The player who gets closer to the total gets points (10 points for exact, 7 points for within five, and 5 points for within 10), whereas the other player gets nothing.

Conundrum
Players have 40 seconds to find make a 9-letter word from the nine randomly-produced letters. The first to buzz in correctly gets 10 points.

On the day

I'm in a room with six other contestants (including the carry-over champion, Esther). We chat for a while, and fill out some paperwork while watching some British Wunderkind reel off one 9-letter word after another on the telly. $*$Gulp$*$. The repetitive music of the show certainly adds to the tension! We then go to a dress rehearsal. We've been told to bring six proper shirts, one for each of the six episodes to be shot that day. It's one-on-one and winner-stays-on, so most of the contestants are pessimistic and don't actually bring six shirts. They don't seem overly competitive, apart from Esther, who has her 'game face' on.

I sit in the studio audience as I watch Esther clobber her first victim of the day. Some guy is telling us when to clap – how irritating (he won't shut up either). Anyway, I'm up next. The other contestants wish me luck, figuring I'd probably need it. I go to the makeup room, where some foundation is put on my face. My hairs are content not to run amok, so they are left alone.

The match

Richard Morecroft's ever-reliable smile and voice begin the show. "Good evening Richard", we say, while our stomachs know full well that we haven't had lunch. David Astle and Lily Serna are introduced as our letter and number

gurus, though we knew perfectly well who they were. Richard asks Esther (a competitive scrabble player) how she got into word games. She used to play Scrabble and Lexicon all the time with her family as a kid. This doesn't bother me though, since I already know how good she is at the letter rounds. Then I'm introduced and asked about my maths exploits – a good match was sure to come.

I'm 'choosing' the letters for the first round. I choose vowels until I get an A and an E (three vowels), then go for all consonants. Straight away I see CLEARING.[2] I can't see any nine-letter word, so I relax. Sure enough Esther matched me. The camera then turns to David, but he's managed no better. Esther chooses four vowels in round two, and my POISED is matched by her COPIED. Yes, I'm level after two letter-rounds! Esther chooses four large numbers for round 3, and I sigh as the target is 600. How lame. We both find $8 \times 75 = 600$.

After the ad break, Esther and I each play a different 7-letter word (there were many). Now David is able to boast a longer word: ADOPTERS. Oh well, still tied. In round 5, I find GLOATED, and wonder why Esther has a pained expression on her face. She produces LIGATED, of which she is suspicious. Alas, it is a word.[3] My luck with the numbers is no better in round 6, when every man and his grandmother find $100 + 1 = 101$.

We get back from the break, and David does a little segment on the origins of the word *pwn*. I'm sure you already know that it comes from trying to type *own* too quickly and missing the 'o'. David finds it quite fascinating that it is now used deliberately, and goes on to discuss the different pronunciations, as well as 1337 speak as a whole.

Round 7 is a miserly letters round, and we both play 6-letter words (I think I played BOASTS). Since round 9 is to be a conundrum, I must surely try to win round 8, which is a numbers round. I choose two bigs and four smalls and see a decent set of numbers. Unfortunately, Lily reads it out wrong and we have to get new numbers! A new set of numbers is produced; to my chagrin, another easy one.

As the final round approaches, I think of all the different suffixes. Surely -ing or -ate or -ion…I don't think of enough though. We're both nervous, and

[2]Good thing I didn't see CARTELING, because it would not have been accepted. The current Macquarie Australian dictionary insists on two Ls.

[3]To ligate is to tie or bind using a ligature. An artery can be ligated, as can musical notes!

the experts congratulate us on what has been a hard-fought and entertaining contest. The conundrum comes, and Esther buzzes in with GLAMOROUS before I am able to even notice the -ous suffix.

I'm given the latest Macquarie Australian dictionary, apparently worth 200 dollars, and I head to the café for a free lunch. Not bad actually. 'Unlucky', my fellow contestants tell me.

The aftermath

I had a good time, and would recommend it to anyone remotely into these sorts of light mental exercises. Be warned though, fellow maths dudes: you only have three numbers rounds with which to draw blood from a wordsmith, as the other six rounds involve letters!

Do check out the show on SBS One, 6pm weekdays, if you haven't already. Season Three is in the works, so check out `http://www.sbs.com.au/shows/lettersandnumbers/about/page/i/2/h/Get-Involved/` if you want to compete or sit in the live audience. The show is huge in Britain, so it may well enjoy increasing popularity here!

— Sam Chow

Solution to puzzles from page 6:

Puzzle 1: The key is realising *all* the boxes are mislabelled. Thus, we need only take one sweet out of the 'mixed' box; if it is mint, then the box must contain all mint sweets (it cannot be mixed), the 'aniseed' box must contain mixed sweets (it cannot be aniseed or mint), and so the 'mint' box must contain aniseed sweets; if it is aniseed, the solution proceeds identically.

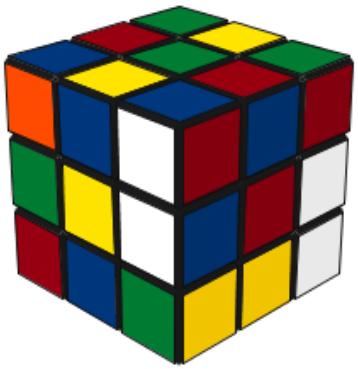
Puzzle 2: There are $169 = 13^2$ digits, cluing us to re-write the code in 13 rows of 13 digits. Removing the commas, we get a skull:

```
0000000000000
00+++++++++00
0++++++++++0
0++++++++++0
0++000+000++0
0++000+000++0
0+++++0+++++0
0++++000++++0
00+++++++++00
000+0+0+0+000
000++0+0++000
000+++++++000
0000000000000
```

God's Number: Solving the Rubik's Cube in the optimal number of turns

A quick question for the Rubik's cubers among you: how many turns of a Cube (quarter or half) are needed to resolve any scrambled starting position? In other words, if an omniscient supreme being took a passing interest in such puzzles, what number of moves would He require, implementing the most efficient possible techniques, to solve any Cube? Fifty? A hundred? More?

Try twenty; each of the Rubik's Cube's 43,252,003,274,489,856,000 positions[1] can be solved with just twenty turns. In other words, the 'distance' of each Cube position from the solved state is at most 20. This remarkable result is as



A Cube of distance 20, reachable via:[2]
F, U, F2, D, B, U, R, F, L, D, R, U, L, U, B, D2, R, F, U2, D2

surprising as its solution has proven illusive; while Ernö Rubik twisted his first Cube back in 1974, the proof that 'God's number' is 20 took another 36 years to complete. And when it was finally demonstrated in July 2010, former University of Melbourne student and Paradox sub-editor John Dethridge[3] was one of those involved in the project. Paradox talked to John to get an insight into the problem, as well as its eventual resolution.

[1]Calculated by noting that there are 8! ways to arrange the 8 corner cubes, of which 7 can be oriented independently in one of 3 ways, and that there are $\frac{12!}{2}$ ways to arrange the twelve edge cubes, of which eleven can be oriented independently in one of 2 ways – this gives $8! \times 3^7 \times \frac{12!}{2} \times 2^{11}$ positions. Thus, the Rubik's Cube's marketing slogan – that there are 'billions of possible positions' – is a massive understatement.

[3]John Dethridge was a member of the MUMS committee in 1998 and 1999, as well as being sub-editor of Paradox in 1999. John has also been a keen participant in the MUMS Puzzle Hunt over the years, with his team winning each of the first three Hunts.

Early attempts

Almost immediately after the commercial release of the Rubik's Cube in 1980, enthusiasts began to search for the quickest and most efficient way to solve this new puzzle. Straightaway, there appeared the fundamental split between 'speed cubists', who seek to solve the Cube in the quickest time no matter how optimal their techniques, and 'purists', who seek to find the most efficient way to solve each position, irrespective of time constraints. Because 'speed cubists' – among them 15 year-old Melbournian Feliks Zemdegs who recently set world records for his quickest solve-time of 6.65 seconds as well as his average of 7.87 seconds[4] – base their technique on pattern recognition and a certain number of memorised algorithms, they regularly take over 40 moves to solve a Cube. For the purist, this simply isn't good enough.

Enter the mathematicians, who began the search for 'God's number' in earnest. There are two broad ways to go about a proof of 'God's number'.

First, one might tackle the problem by trying to efficiently solve each position individually. Indeed, since the early days of the Cube, computer algorithms have existed that produce efficient, or even the most efficient, solution for individual positions. Thus, in theory, to find 'God's number's, it would be sufficient to feed all possible positions into such an algorithm.

The catch: with over 43×10^{19} possible positions, the computer run-time would be overwhelming; Tomas Rokicki calculated that it would take 1 million computers 100,000 years to complete such a solution even using clever case-reduction techniques.[5]

The alternative is to tackle the Cube as does any solver: to break the solution down into smaller stages, and then determine the maximum number of turns required to push through each of these stages in the 'worst-case scenario'. For most beginner cubers, such a break-down is based on the three layers of the Cube, and usually goes something like: (1) position a 'cross' on the base layer; (2) solve the rest of the base layer; (3) solve the 2nd layer; (4) position the edges on the 3rd layer; (5) re-orientate the edges on the 3rd layer; (6) position the corners of the 3rd layer; and (7) re-orientate the corners of the 3rd layer.

For a beginner solver using such a basic break-down, the minimum number of moves will typically be around 100. The task of finding more efficient so-

[4]See http://en.wikipedia.org/wiki/Feliks_Zemdegs.

[5]http://www.springerlink.com/content/q088143tn805k124/fulltext.pdf.

lutions becomes the task of determining innovative ways to break-down the problem, and then to develop efficient algorithms to push through each stage. However, in contrast to the above method, there is no guarantee that such a technique will produce optimal solutions for every position.

Very quickly, mathematicians began producing a string of upper-bounds for 'God's number' based on innovative break-downs that involved group theory. The first major breakthrough was by Morgan Thistlethwait, who in 1981 set the bound at 52 using a four-step break-down that involved shifting the Cube through 4 nested subgroups of the group of all Cube positions.[6] By 1992, the bound had been reduced to 37 using variations on this technique.

The next significant breakthrough was a two step-algorithm developed by Herbert Koceimba in 1992, that sought to: (1) reduce any Cube position to an element of a particular subgroup H;[7] (2) solve this element of H. In 1995, Koceimba's algorithm was adapted by Michael Reid to slash the bound to 29.[8]

At the same time, the search was on to find a lower-bound; that is, to find positions of the Cube that are 'hardest' to solve. After the lower bound had stagnated at 18 for many years, Michael Reid was the first to raise this to 20, demonstrating in 1995 that the so-called 'superflip' position[9] requires 20 moves to solve.[10] Interestingly, Michael Reid conjectured at the time that the lower-bound would eventually be raised even higher...

It would take until 2005 for an improvement to be made on Michael Reid's upper-bound of 29, but when the breakthrough came the bound quickly tumbled: from 28 in 2005 to 27 in 2006, and then to 26 in 2007, until Tomas Rokicki and John Welborn managed to reduce it to 22 in 2008, all using modifications of Koceimba's algorithm. At this point it was already suspected by most that 'God's number' was 20, and so the stage was set for one final push to reduce the lower-bound accordingly.

[6]The subgroups are the groups generated by {L,R,F,B,U2,D2}, {L,R,F2,B2,U2,D2}, {L2,R2,F2,B2,U2,D2} and I, where {L,R,F,B,U,D} generates the group of all Cube positions (using the notation defined above). For more details see http://www.jaapsch.net/puzzles/thistle.htm.

[7]H is the group generated by {L,R,F,B,U2,D2} using the notation identified above, ie. the outer layer of Thistlethwait's nested subgroups. For more details see http://www.jaapsch.net/puzzles/compcube.htm#kocal.

[8]http://www.math.rwth-aachen.de/~Martin.Schoenert/Cube-Lovers/michael_reid__new_upper_bounds.html.

[9]This position has each of the mini-cubes in its original position, with each edge cube flipped over.

[10]http://www.math.rwth-aachen.de/~Martin.Schoenert/Cube-Lovers/michael_reid__superflip_requires_20_face_turns.html.

The breakthrough

The team who would ultimately be successful in resolving 'God's number' comprised of Tomas Rokicki, a programmer from California, Herbert Kociemba, a maths teacher from Germany, Morley Davidson, a mathematician from Kent State University, and John Dethridge, former University of Melbourne student and current software engineer at Google.

As noted above, Rokicki and Kociemba had been heavily involved in previous efforts at lowering the upper-bound. Indeed, since his demonstration of the 22-bound, Tomas had continually been improving his algorithm, with input from Herbert, Morley and John, who has been friends with Tomas even since first meeting at a computer programming competition many years ago. The team's hope was that the combination of more efficient algorithms and fasted computer processing speeds would soon give them a chance to complete the computations for the 20-bound in a reasonable time.

To recall, the team's approach was again based on Koceimba's technique of breaking the solving of a Cube into two stages. In essence, the team would reduce the problem into sub-problems, each corresponding to a coset of the subgroup H.[11] This technique allowed the team to break the problem into 2,217,093,120 sub-problems (corresponding to the cosets of H), each consisting of 19,508,428,800 positions (the number of Cube positions within each coset).

The number of coset elements was further reduced by symmetry arguments: because the solution to a Cube is identical no matter which of the 24 orientations you hold a Cube, or whether the Cube is looked at through a mirror, the number of sub-problems could be cut by a factor of about 48.

The team then made use of several techniques to optimise the algorithms used for solving each coset. While some of these techniques are complex, one of the more basic was the appreciation that the problem did not require the determination of any solution of less than 20 moves, so once the algorithm could solve a particular coset within 20 moves this coset could be discarded, irrespective of whether it needed 20, 19, 18 or less turns to complete.

Despite these efficiencies, the team was still in need of an extraordinary amount of computing power to complete the demonstration (in the thousands of CPU years). And, as any mathematician who has sought to be the first to prove a

[11] See footnote 5 for details on how to construct H.

result will know, time was of the essence.

This is where John's involvement in the project became critical. John works as an engineer for Google, and so had ready access to vast computing power. As John tells it, whenever the team made a breakthrough in improving the efficiency of the algorithms, John would ensure that they calculated the CPU time still needed for computation, waiting for it to fall far enough to be manageable.

Once the CPU time was finally attainable (the final figure was estimated by the team to be around 35 million CPU hours in a modern computer, or around 4,000 CPU years), John spoke with Google's head of research, who was supportive of the team's project (as John puts it, there are a lot of maths and Rubik's Cube enthusiasts at Google), and volunteered some of Google's resources.

John then put his expertise in computer systems to use in setting up the team's algorithms to run across multiple computers simultaneously, slashing the overall time needed for the computation. Once John had set up Google's computers to run the algorithms in parallel, the computation was completed in just a few weeks.

For completeness John's team also compiled a table showing the number of Cube positions, out of the approximately 4.3×10^{19} in total, of each 'distance' from the solved state[12] – note that the latter values are not known precisely:

1	18
2	243
3	3,240
4	43,239
5	574,908
6	7,618,438
7	100,803,036
8	1,332,343,288
9	17,596,479,795
10	232,248,063,316

11	3,063,288,809,012
12	40,374,425,656,248
13	531,653,418,284,628
14	6,989,320,578,825,358
15	91,365,146,187,124,313
16	$\approx$ 1,100,000,000,000,000,000
17	$\approx$ 12,000,000,000,000,000,000
18	$\approx$ 29,000,000,000,000,000,000
19	$\approx$ 1,500,000,000,000,000,000
20	$\approx$ 300,000,000

* * *

Exactly 30 years after the Rubik's Cube was first commercialised, and 15 years after Michael Reid had first proved that the 'superflip' position required 20

[12] http://cube20.org.

moves to solve, each of the Cube's 43,252,003,274,489,856,000 positions have been shown to be solvable in at most 20 turns.

And given that speed cubers tend to achieve at least 5-6 turns a second, this suggests that the optimum time to which they should be aspiring is well under 4 seconds. Something for Feliks Zemdegs to aim for, perhaps?

— Stephen Muirhead

Solution to puzzles from page 6:
Puzzle 3: The key is to make use of the temperature of the bulb. Turn the first switch on, and leave it for half and hour. Then turn it off, and turn the second switch on. Immediately open the door; if the light is off and bulb is hot, the first switch activates the light; if the light is on and the bulb is hot, it is the second switch; if the light is off and the bulb is cold, it is the third switch.
Puzzle 4: Turn over both sand clocks. When the four-minute clock is empty, turn it back over. When the seven-minute clock is empty, turn it back over. When the four-minute clock is empty again, eight minutes have elapsed. At this point, there is one minute of sand in the seven-minute clock; so turn it over to time the last minute.
Puzzle 5: There are only eight sets of three positive integers that have product 36, six of which have a distinct sum; the ages cannot be one of these six sets, because then there would have been no need for the final bit of information. The remaining two sets are $1, 6, 6$ and $2, 2, 9$. Only one of these sets is consistent with the existence of an 'eldest' daughter (although, it is true that there might be two daughters aged 10 months apart...). Thus, the ages are 2, 2 and 9.
Puzzle 6: Indicating one of the doors, the stranger should ask one guard: 'If I asked the other guard: "Is this the door to freedom?", what would he say?'. If the guard says yes, he should take the opposite door. If the guard says no, he should take this door. The question works because it captures exactly one lie and one truth, irrespective of which guard is asked.

The *Kryptos* Puzzle

Kryptos is a sculpture by Jim Sanborn located on the grounds of the Central Intelligence Agency (CIA) Headquarters in Langley, Virginia.[1] Unsurprising given its location, *Kryptos* is not your average sculpture: it contains encrypted messages, embossed on its surface by Sanborn with the held of retired CIA employee Ed Scheidt. Since *Kryptos* was dedicated in November 1990, cryptologists, both professional and amateur, have been clambering to decipher the codes, with limited success. Although *Kryptos* has always been famous amongst the intelligence community, its notoriety has recently crossed over to the mainstream through Dan Brown's 2009 best-selling book *The Lost Symbol*, in which it formed a central tenet of the plot.[2]

The *Kryptos* puzzle contains two parts, widely believed to be the cipher on one side and the key on the other. The code, in turn, has apparently been divided into four distinct sections (K1, K2, K3 and K4), with a different cipher applied to each one. It is also widely expected that *Kryptos* is a 'puzzle within a puzzle': only after the four sections have been deciphered will the 'meta puzzle' become apparent.

[1] Due to its location, it is effectively inaccessible to the general public.

[2] There are also two references to *Krpytos* on the dust jacket of the US version of *The Da Vinci Code*. More details of this and other references are here: http://en.wikipedia.org/wiki/Kryptos#Pop_culture_references.

To date, only three of the four sections have been deciphered. In 1999, James Gillogly, a computer scientist from Southern California, was the first person to publicly announce solving the first three sections. After Gillogly's announcement the CIA revealed that their analyst David Stein had solved the same sections in 1998 using pencil and paper methods, although this fact was only made known to the intelligence community. Finally, the National Security Agency (NSA) revealed in 2005 that a team of its members had also solved the first three section using a computer in late 1992.

Yet the fourth section has remained stubbornly undecipherable. On the 20th anniversary of the puzzle in November 2010, Jim Sanborn, apparently frustrated by the lack of progress on *Kryptos*, decided to release a clue for the fourth section: the characters 'nypvtt' become 'Berlin' once decoded.[3] This revelation has spurred renewed interest in *Kryptos*, which still provides a diversion for current CIA employees over twenty years after its inauguration.

The rest of this article will explain the techniques used to solve the first three sections of *Kryptos*, providing a full solution at the end.[4]

Vigenère Cipher

The first two sections of *Kryptos* (K1 and K2) use a slightly modified Vigenère tableau for their encryption.[5] The Vigenère cipher encrypts alphabetic texts by using several different Caesar ciphers[6] based on the letters of a keyword. Encryption is done using a table of alphabets, called a *tabula recta*, Vigenère square, or Vigenère table. The table consists of 26 rows of all the possible Caesar ciphers.

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

A regular Vigenère table.

[3] http://www.guardian.co.uk/world/2010/nov/21/jim-sanborn-kryptos-puzzle-cia.

[4] Needless to say, there will be SPOILERS.

[5] Those interested in seeing the actual solution and the modified tableau for the first two sections of *Kryptos* can look at the last section of this article or go here: http://web.archive.org/web/20071116100808/http://filebox.vt.edu/users/batman/kryptos.html.

[6] A Caesar cipher replaces each letter of the original 'plaintext' message with a letter a fixed number of positions along in the alphabet. Eg. A shift of four replaces `A` with `E`, `B` with `F`, etc.

For example, say we want to encrypt the plaintext RETREATIMMEDIATELY using the keyword REVERSE. First, REVERSE is repeated until it matches the length of the plaintext, like so REVERSEREVERSEREVE. We then use the Vigenère table to produce the encrypted text by going to the row specified by the key and the column specified by the plaintext. For instance, to encrypt the first letter of the message we go to row R and column R of the table to get I, for the next letter we use row E and column E giving I, then row V and column T giving O, etc.[7] The final result should be:

Plaintext:	RETREATIMMEDIATELY
Key:	REVERSEREVERSEREVE
Ciphertext:	IIOVVSXZQHIUAEKIGC

Decryption can be done using a Vigenère table by going to the row specified by the key letter, and finding which column the ciphertext letter belongs to, which will be the corresponding plaintext letter. For example, for the first letter we have the key letter R and the ciphertext letter I, so we go to row R and find that I appears in column R, so R is the first plaintext letter.

It is also possible to view the Vigenère cipher algebraically, where the letters A–Z are taken to be the numbers 0–25 and calculations are done modulo 26. Now encryption and decryption of the ith letter, where C stands for ciphertext, P stands for plaintext, and K stands for key, can be written like this:

$$C_i \equiv (P_i + K_i) \pmod{26}$$

$$P_i \equiv (C_i - K_i) \pmod{26}$$

Now if we want to encrypt the first letter of the above example, we add $\mathtt{R} \equiv 17$ with $\mathtt{R} \equiv 17$ to get $34 \equiv 8 \pmod{26}$ which gives the letter I. While if we want to decrypt the last letter we subtract $\mathtt{E} \equiv 4$ from $\mathtt{C} \equiv 2$ to get $-2 \equiv 24 \pmod{26}$ which gives the letter Y.

Transposition Cipher

The third section of *Kryptos* (K3) is a transposition cipher where letters or groups of letters in plaintext are shifted around systematically to produce the

[7] Since this Vigenère table is symmetric, it doesn't actually matter whether we use the rows determined by the key letters and the columns determined by the plaintext letters or vice versa.

ciphertext. This section will give some examples of transposition ciphers.[8]

Rail Fence Cipher The Rail Fence cipher gets its name from its method of encryption, which involves writing the plaintext on the successive 'rails' of an imaginary fence, starting diagonally downwards and then going diagonally upwards when it gets to the bottom, and then diagonally down again from the top, etc. The ciphertext is then read off the rows. For instance, if I wanted to encode the message `ATTACK THE GRID AT NIGHT` using three 'rails', I would write out:

```
A . . . C . . . E . . . D . . . I . . .
. T . A . K . H . G . I . A . N . G . T
. . T . . . T . . . R . . . T . . . H .
```

Which gives me the ciphertext: `ACEDITAKHGIANGTTTRTH`, which can be decrypted by replacing the text back onto the three imaginary "rails" in such a way that they make the original zig-zag pattern.

Route Cipher In a route cipher, the plaintext is written out in a grid of given dimensions (possibly with extra letters if the original plaintext does not fit) and is then read off in a pattern given by a key. For example, if I can use the plaintext from before and write it into a 3×7 grid, with an extra `X` to fill the space:

```
A T K E I T G
T A T G D N T
T C H R A I X
```

The key could be 'spiral inwards clockwise from the top left', which gives the ciphertext: `ATKEITGTXIARHCTTATGDN`. This can be decrypted by replacing the letters into the original grid in the order the key specifies.

Route ciphers have many more keys than rail ciphers, with the larger ones having more routes than can be enumerated by current computers, although an ill-chosen route can leave large chunks of plaintext or reversed plaintext which will give clues about the route.

[8]Section three of *Kryptos* seems to be a column transposition. Examples of how to solve it can be found at http://elonka.com/kryptos/part3.html and http://www.elonka.com/kryptos/mirrors/daw/steinarticle.html as well as in the last section of this article.

Columnar Transposition In a columnar transposition, the message is written out in rows of fixed length, and then the columns are chosen in some order. The order of the columns and length of the rows depends upon some keyword. For instance, if we choose the word `COWS`, with the permutation defined by alphabetical order, we get rows of length four and columns in the order "1 2 4 3". If there are spare places, then one can choose to either fill them with extra letters, called 'nulls', or leave them blank.

Now, if we use the keyword `COWS` to encrypt the same message as above, i.e. `ATTACK THE GRID AT NIGHT`, we have:

```
1  2  4  3
A  T  T  A
C  K  T  H
E  G  R  I
D  A  T  N
I  G  H  T
```

which produces the ciphertext `ACEDITKGAGAHINTTTRTH`.

To decrypt, you work out the lengths of the columns by dividing the length of the message by the length of the keyword, and then write the message out in columns before reordering them to form the original message.

Double Transposition A single columnar transposition is vulnerable to attack by having its column length guessed, and then writing out the message in columns in a jumbled order and looking for anagrams. It can be strengthened by a second columnar transposition, with the same or a different key.

For example, the result of the single columnar transposition above could be encrypted again by the word `BEAK`, which gives an order of '2 3 1 4'.

```
2  3  1  4
A  C  E  D
I  T  K  G
A  G  A  H
I  N  T  T
T  R  T  H
```

This gives us `EKATTAIAITCTGNRDGHTH` as the ciphertext.

Myszkowski Transposition A Myszkowski transposition uses a keyword with recurring letters, where columns of the plaintext corresponding to a unique letter are transcribed downwards, while those corresponding to the same recurrent letter are transcribed left to right. For instance, if we were to encrypt `ATTACK THE GRID AT NIGHT` with the keyword `POTATO`, which gives us and order of '3 2 4 1 4 2', we get:

```
3  2  4  1  4  2
A  T  T  A  C  K
T  H  E  G  R  I
D  A  T  N  I  G
H  T
```

This gives us the ciphertext `AGNTKHIAGTATDHTCERTI`. Decryption takes place as usual; find the lengths of the columns and then fill them in.

K4: The unsolved section

For those interested in K4, here is a list of some of things already tried:[9]

- Morse Code
- Palindromes
- Placement of rocks and other elements in the courtyard
- Shadows and sundials
- Egyptian references
- Magnetism
- Folding one half of the sculpture on top of the other
- Connecting the two halves into a Jefferson Cypher Cylinder
- WWII Enigma machine
- Holding a candle up to the sculpture and observing light rays
- Combining the methods of 1-3 to solve K4
- Kryptos looks like a flag, an S, or printer paper

For those of you who wish to tackle something a little easier than *Kryptos*, or are looking to practice before making a big attempt, there is the MUMS puzzle hunt, currently scheduled to take place the week before Easter (10–15 April). You can keep an eye on it by visiting our website: `mums.org.au/puzzlehunt/`.

[9] Taken from the Kryptos FAQ: http://www.elonka.com/kryptos/faq.html.

SPOILER: The solution to K1, K2 and K3

This is a summary of David Stein's pen and paper solution to K1, K2 and K3.[10]

David Stein's first observation was that the sculpture was divided into two: a coded message of 865 characters interspersed with four question marks, and a modified Vigenère table, with `KRYPTOSABCDEFGHIJLMNQUVWXZ` in place of the normal alphabet.

Using frequency analysis on letters in each row, Stein then determined that different sections were encoded differenly; there is a dramatic change in almost all of frequencies between rows 1–14 and rows 15–28. Stein thus split the code into two sections of 14 rows each. He, in turn, split the top section into Parts I, II and III – corresponding to K1 and K2 – and the bottom section into Parts IV and V – corresponding to K3 and K4 – based on the question marks.

K1 and K2
Stein decided to tackle Part II first. Frequency analysis – English has characteristic letter frequencies which are difficult to disguise – showed that K2 had a much flatter distribution than regular English, indicating a polyalphabetic substitution (as the distribution of several alphabets averages out when combined). He therefore decided to make use of the modified Vigenère table inscribed on *Kryptos*.

To make use of the table, Stein needed to determine the length of the key word. This would allow the code to be broken up into its constituent 'monoalphabets' so that analysis can be carried out on each separately, determining which Vigenère alphabet it belongs to. To do this, Stein used the 'index of coincidence', or IC, given by: $\frac{\sum_{i=1}^{c} n_i(n_i-1)}{N(N-1)}$ where c is the number of letters in the alphabet, N is the length of the text, and n_1 through n_c are the observed letter frequencies in the text. The IC is the probability that any two randomly chosen letters from the text will be the same. For English (or a Caesar cipher) this probability is around 0.67, with random text having an IC of $1/26 \approx 0.0385$. To implement IC, Stein divided the code into two alphabets, then three, then four etc. and calculated the average IC for each. He discovered that the IC for eight alphabets was 0.63 – significantly higher than the others – which made it a very likely key length.[11]

[10] For a full description see: http://www.elonka.com/kryptos/mirrors/daw/steinarticle.html.

[11] Another method for finding the code length is the Kasiski examination, which involves looking for repeated groups of letters in the ciphertext, as these may indicate that the same words

Now Stein needed to determine which Vigenère alphabet each monoalphabet belonged to. The scarcity of letters prevented him from using a straightforward frequency count.[12] After months of stagnation, Stein proceeded by writing out all possible encodings of the monoalphabets, and looking for likely letter combinations between them. To quicken this, he rejected encodings contained many uncommon letters. To quantify this, Stein used the log sum of the English letter frequencies of the letters in each of the encodings of the column; eg. for the column `DDFIQGNGXJJZDFSD`, the frequency of 'D' is 4.4 per 100 letters, 'F' is 2.8, 'I' is 7.4, giving a log sum of $\log(4.4) + \log(4.4) + \log(3.8) + \log(7.4) + \ldots = 7.3$. Stein used the log sum because the uncommon letters B, J, K, Q, X, and Z have negative log frequency values, which reduce more dramatically the overall scores of the monoalphabets containing them.

Stein began his search for likely combinations at the beginning; he found that the first decoded monoalphabet had the highest log sum when it began with 'R' (25.2), 'T' (23.7) and 'O' (4.8). 'O' starts a word on average 7.2 times per 100 words, 'R' 3.1 times, and 'T' 16 times, making T a good choice for a first decoded letter. Stein then looked at which second and third letters would give him 'THE' as a starting word, since it is a very common word in English. The log sum frequency for the decoded monoalphabet with 'H' in second position was 29.4, and for the 'E' was 30.5, making them likely candidates for the plaintext. More importantly, there were no obvious impossible combinations of letters when these monoalphabets were brought together.[13] Stein instead found signs he was on the right track, such as 'AND', the suffix '-TION', and the combination 'KNO', which made it extremely likely the next letter would be a 'W'. Stein then used the decoded fourth monoalphabet that placed a 'W' in the required position, and similarly decoded the rest.

Stein had cracked Part II, and his attempts to decode Part III with the same key also proved successful (since Parts II and III are both in K2.) Moreover,

were encrypted using the same part of the key. For instance, the letters 'DQM' are found at the start of Part II, and again at characters 9–11; a distance of eight characters. Assuming the letters 'DQM' are still the same when converted to plaintext, this means that the key must have length eight, four, two or one. ICs can then be calculated for each of these possibilities.

[12] Otherwise, he could have used the fact that the most common letter was likely to correspond to plaintext 'E'.

[13] Such impossible combinations include 'AAA' and 'Q' without a 'U'.

even though Part I was encoded differently, by recomputing ICs and using a different key length, he was able to crack this too.

Part IV

Stein began his analysis of Part IV with a frequency count, revealing similarities to normal English that normally indicate that Part IV is a transposition cipher. After some deliberation, Stein decided to treat the text as a columnar transposition. Stein thus needed to figure out the number of columns and rows. Since the column lengths could be either be B or $B-1$ (if the last row of a message is not completely filled in there will be columns which are one letter shorter than the other ones), Stein had the relation $(B-1)x + By = 336$, where x is the number of pieces of length $B-1$, y the number of length B, and 336 the number of characters in Part IV. Since x, y and B must be integers, there were only a finite number of solutions.

Stein then noted that Part IV begins with the word 'END', and wondered if it was a clue that this was the final column in the grid. If so, the columns had to either be either a mix of length 3 and 4, or all length 3. Stein also intuitively felt that the columns should be short, because he came up with too many problems when he tried to form horizontal words using columns of long lengths.

After many months, Stein settled on $B = 4$ as a working hypothesis. He then needed to decide how many columns were of length 4 and how many of length 3. Since his hypothesis was that the first three letters were a column, Stein felt that the final three letters would also be a column due to symmetry. From the formula, he also knew that only certain solutions were feasible: $(x = 0, y = 84), (x = 4, y = 81), (x = 8, y = 78) \ldots (x = 112, y = 0)$. This left him 28 solutions to check; trying them in order, $(x = 8, y = 78)$ proved correct.[14]

Finally, Stein rearranged the columns using a 'diagraphic frequency table', which depicts how often, on average, any two letters occur next to each other. For instance, 'YO' occurs 0.64 times per 1000 letter pairs and 'AH' occurs 0.13 times. By summing these frequencies for each combination of columns, he calculated which were most likely to occur next to each other and so fit them back together like a jigsaw puzzle. Stein had cracked K3!

— Wvj Rasf
— *Kry Ptos*

[14]The columns of length three are evenly distributed, with eleven columns of length four between each of them, except for the middle two, which have twelve columns of length four between them.

Great Lives

> *I have been surprised at finding how often insanity or idiocy has appeared among the near relatives of exceptionally able men. Those who are over eager and extremely active in mind must often possess brains that are more excitable and peculiar than is consistent with soundness. They are likely to become crazy at times, and perhaps to break down altogether.*
>
> —Francis Galton[1]

What constitutes a great life? Is it one filled with achievements, unusual abilities, and extraordinary events? Or is it one marked by great conflict both without and within, indelibly etched by moments of ecstasy and tragedy? Perhaps a great life entails much of the aforementioned and yet much, much more, for the life of a great person is naturally difficult to pin down and classify. I intend to discuss the lives of five such great mathematicians,[2] with less emphasis on their mathematical prowess and more on what else filled their lives.

Sadly, mathematics tends to be taught devoid of the history behind humanity's great leaps and bounds in the eternal pursuit of knowledge, much to our detriment when we find ourselves cramming concept after concept before an examination, unaware of the beautiful narrative holding everything together. We are but creatures of association, and it is by associating the achievements of these mathematicians with their personal lives that I hope you find this article to be useful.

Archimedes of Syracuse (c. 287 – 212 BC)

Few details of his life are known, yet he is ranked among the greatest of mathematicians for his achievements in antiquity. A Greek physicist, engineer, inventor, and astronomer to boot, his face adorns the obverse of the Fields Medal for outstanding achievement in mathematics,[3] encircled by a quote attributed to him:

Transire suum pectus mundoque potiri.[4]

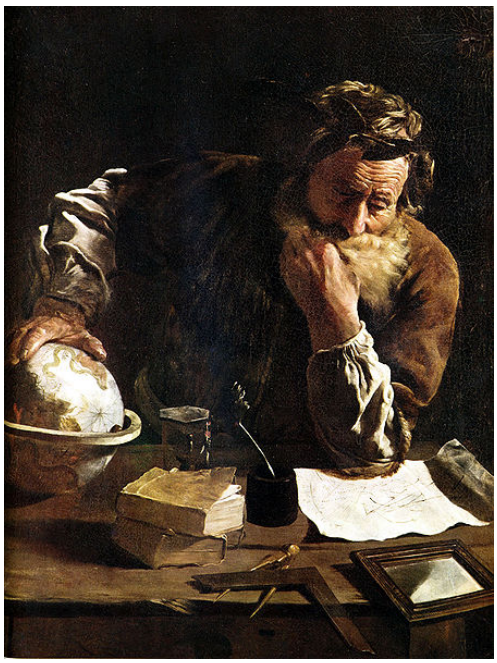
[1] Francis Galton, *Hereditary Genius* (1892), 9–10.

[2] I had originally intended to describe the lives of ten such persons, but found the length of the resultant article to be excessive. The five individuals omitted but no less worthy of inclusion were Gottfried Leibniz, Leonhard Euler, Carl Friedrich Gauss, Karl Pearson, and Srinivasa Ramanujan.

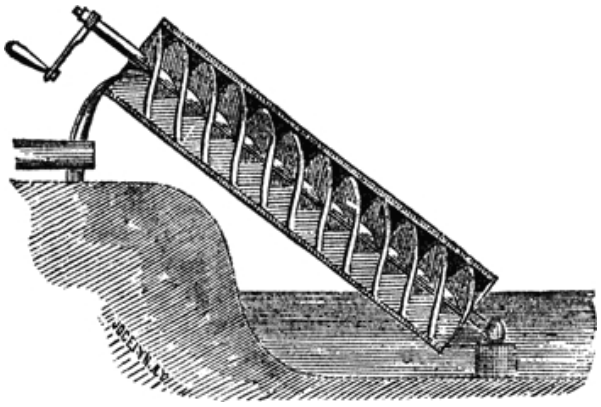
[3] Described as 'The Nobel Prize for Mathematics' for its prestige, although only mathematicians not yet forty years of age are eligible.

[4] Latin for 'Rise above oneself and grasp the world.'

For physics, he laid the foundations of hydrostatics, statics, and the principle of the lever. The most widely known anecdote about Archimedes is that upon discovering the law of buoyancy in hydrostatics, he leapt from his bath and absent-mindedly ran naked down the street shouting 'Eureka!' For mathematics, he is best known for his contributions to the theory of π, but it is not known how he celebrated his work on that most famous number of mathematics. It is to him that we owe the familiar approximation $\frac{22}{7}$ for the value of π;[5] he estimated it to be bounded between $\frac{223}{71}$ and $\frac{220}{70}$. He also once concluded that the number of grains of sand required to fill the universe would be 8 vigintillion, that is, 8×10^{63}.



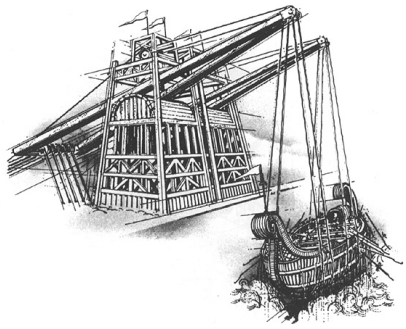
Interestingly, Archimedes was better known in his time for his inventions rather than his mathematical writings. He designed the screw which now bears his name, a cylinder containing a revolving screw-shaped blade which raised water efficiently; it is still used today for pumping liquids and granulated solids. The odometer, which indicates the distance travelled by a vehicle, is also credited to him for he invented a cart with a gear mechanism that dropped a ball into a container after each mile travelled.



The Archimedes screw

[5]Hence Pi Approximation Day on July 22 each year.

He also designed weapons of war for the defence of Syracuse, his city of birth. Most famous among them are the Claw of Archimedes and the Archimedes Heat Ray. The claw consisted of a large metal grappling hook suspended from a crane-like arm. The claw would be dropped onto an attacking ship, and then the arm would swing upwards, lifting the ship out of the water to almost certain doom.[6] The heat ray consisted of mirrors used to focus sunlight on approaching ships, causing them to catch fire.[7] However, its credibility has been questioned since the Renaissance. It was rejected by the natural philosopher René Descartes as false but modern attempts to recreate the heat ray using only materials available to Archimedes have yielded mixed results.[8]



The Archimedes Claw

Archimedes died when Roman forces captured the city of Syracuse after a two-year siege. According to the Roman historian Plutarch, Archimedes refused to stop contemplating a mathematical diagram to meet the victorious Roman general Marcellus, enraging the Roman soldier commanding him, who killed Archimedes with his sword. This was against the general's orders not to harm Archimedes, whom he considered a valuable scientific asset.

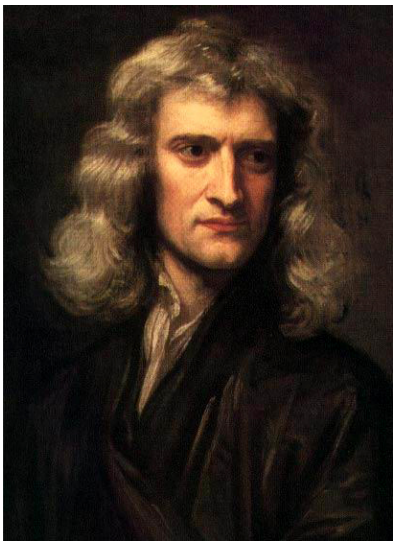
The tomb of Archimedes, the likeness of which is found on the reverse of the Fields Medal (see below), carried a sculpture illustrating his most favourite proof: Given a sphere inscribed within a cylinder, the sphere has two thirds of the volume and surface area of the cylinder.

[6]In 2005, the television documentary *Superweapons of the Ancient World* built a version of the claw and concluded that it was a feasible ancient weapon.

[7]It also provides the inspiration for the laser-shooting mirror towers in the Archimedes scenario of *Age of Empires: Rise of Rome*.

[8]In 1973, Ioannis Sakkas successfully ignited a mock-up of a Roman ship 50m away within a few seconds using 70 copper-coated mirrors (1.5 x 1 m) , while in 2005, an MIT group only managed to do so after 10 minutes using 127 (30 cm) square mirror tiles 30m away. The latter repeated the experiment the following year for the television show *Mythbusters*, declaring the myth 'busted' because of the length of time required.

Isaac Newton (1643 – 1727)



An English physicist, mathematician, astronomer, natural philosopher, alchemist, and historian, Newton deserves much of the credit for advancing the Scientific Revolution. His *Philosophiæ Naturalis Principia Mathematica*[9] helped establish most of classical mechanics, which dominated science's view of the physical universe for the next three centuries. Newton himself often told the story that he was inspired to formulate his theory of gravitation by watching an apple fall from a tree.[10]

Born prematurely three months after the death of his father and small, Newton's mother reportedly said that he could have fit inside a quart mug.[11] When he was three, his mother remarried and went to live with her new husband, leaving her son in the care of his maternal grandmother. The young Isaac disliked his stepfather, and his mother for marrying him, as revealed by an entry in a list of sins he committed up to the age of nineteen:

> *Threatening my father and mother Smith to burn them and the house over them.*[12]

He also suffered from several nervous breakdowns in his life and was known for great fits of rage towards anyone who disagreed with him. The latter was particularly the case when he became involved in a dispute with Leibniz over who developed infinitesimal calculus, albeit with very different notations. Together with other members of the Royal Society of which Newton was a member, he accused Leibniz of plagiarism and influenced the Royal Society to publish a study claiming Newton was the true discover and Leibniz a fraud. This controversy marred the lives of both Newton and Leibniz until the latter's death.

[9] Latin for 'Mathematical Principles of Natural Philosophy'.

[10] Some cartoons have gone further to suggest that the apple actually hit Newton's head, but this is unsubstantiated.

[11] Capacity $\approx$ 1.1 L.

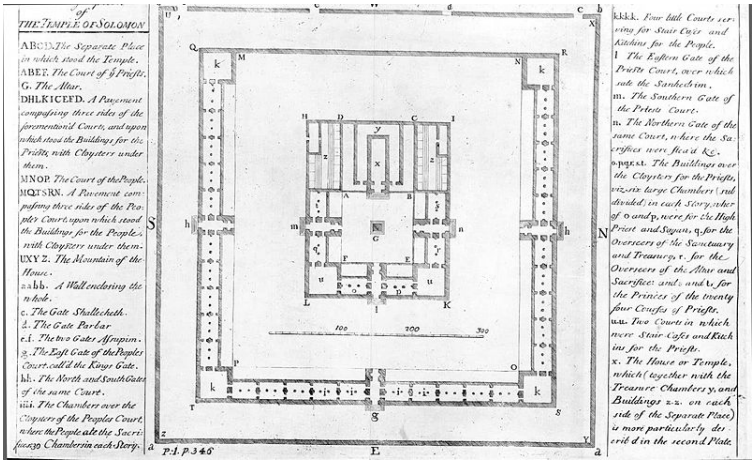
[12] I B Cohen, *Dictionary of Scientific Biography* Vol 11 (1970), 43.

While Newton is mainly associated with science and mathematics, he actually wrote more on Biblical hermeneutics (interpretation theory) and occult studies (studies of the hidden) throughout his lifetime. A highly religious yet unorthodox Christian, he warned against using his discoveries of the laws of motion and universal gravitation to create a mechanistic Universe akin to a great clock:

> *Gravity explains the motions of the planets, but it cannot explain who set the planets in motion. God governs all things and knows all that is or can be done.*[13]

He also attempted to extract scientific information and hidden messages from the Bible, placing the crucifixation of Jesus Christ at 3 April, AD 33 and estimating that the world would end no earlier than AD 2060. Of the latter he said:

> *This I mention not to assert when the time of the end shall be, but to put a stop to the rash conjectures of fanciful men who are frequently predicting the time of the end, and by doing so bring the sacred prophesies into discredit as often as their predictions fail.*[14]



Newton's diagram of part of the Temple of Solomon, taken from Plate 1 of *The Chronology of Ancient Kingdoms*.

[13] J H Tiner, *Isaac Newton: Inventor, Scientist and Teacher* (1975).

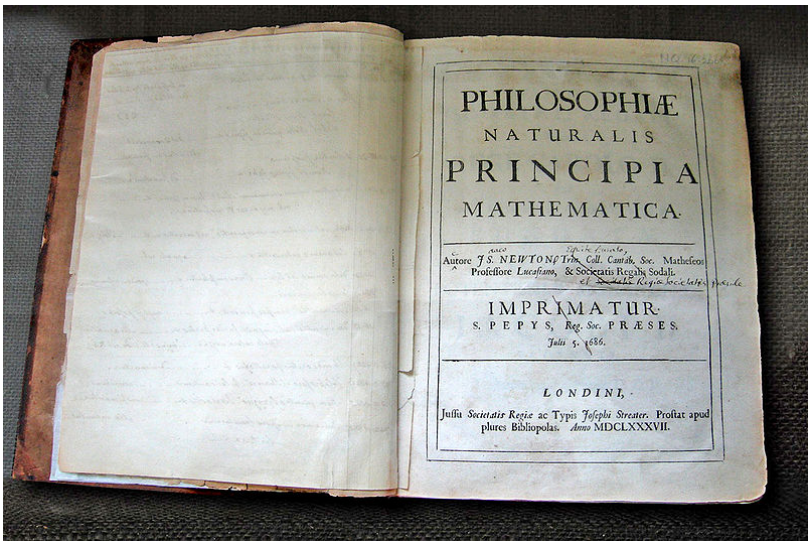
[14] *Papers Show Isaac Newton's Religious Side, Predict Date of Apocalypse*, Associated Press, 19 June 2007.

Newton was also once made warden of the Royal Mint, where he ruthlessly pursued counterfeiters until they were hanged, drawn, and quartered, no matter how difficult it was to catch the worst offenders. He also bears responsibility for naming the seven colours of the rainbow. He originally named only five primary colours: red, yellow, green, blue, and violet, but later included orange and indigo, giving seven colours simply so that they could be analogous to the number of notes in a musical scale.[15]

Thus, it seems that Newton valued rediscovering the occult wisdom of the ancients more than his scientific work. Indeed, after purchasing and studying Newton's works in alchemy in 1942, the British economist John Maynard Keynes concluded that 'Newton was not the first of the age of reason, he was the last of the magicians.'[16] Nonetheless, the English poet Alexander Pope wrote this famous epitaph in Newton's honour:

Nature and nature's laws lay hid in night;

God said 'Let Newton be' and all was light.

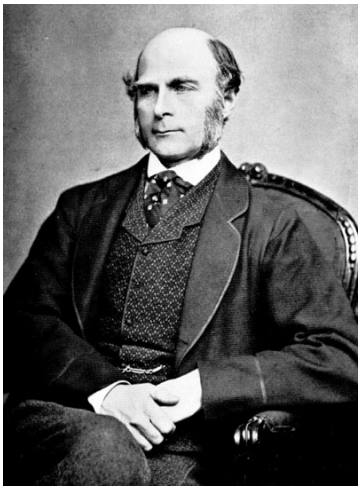

PHILOSOPHIÆ
NATURALIS
PRINCIPIA
MATHEMATICA
Autore J. S. NEWTONO Trin. Coll. Cantab. Soc. Matheseos Professore Lucasiano, & Societatis Regalis Sodali.
IMPRIMATUR.
S. PEPYS, Reg. Soc. PRÆSES.
Julii 5. 1686.
LONDINI,
Jussu Societatis Regiæ ac Typis Josephi Streater. Prostat apud plures Bibliopolas. Anno MDCLXXXVII.

Newton's own first edition copy of *Principia Mathematica*, with hand-written corrections for the second edition.

[15]Thus starting the ceaseless confusion between violet and indigo among young children.

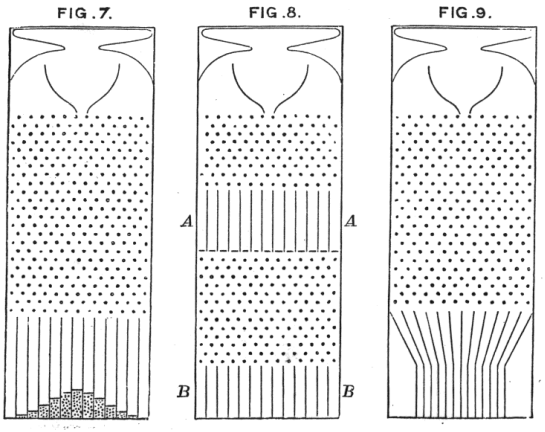
[16]John Maynard Keynes, 'Newton, The Man', *The Collected Writings of John Maynard Keynes Volume X* (1972), 363–4.

Francis Galton (1822 – 1911)



A prolific English Victorian polymath who produced over 340 papers and books throughout his lifetime, Francis Galton was Charles Darwin's half-cousin. In mathematics, he is known for his contributions to statistics: he created the statistical concept of correlation, promoted regression towards the mean, and came up with the concepts of standard deviation and the regression line. He also invented the Quincunx, a pachincko-like bean machine which he used to demonstrate the central limit theorem and normal distribution.

By many accounts a child prodigy, Galton was reading by the age of two; at age five he knew some Ancient Greek, Latin, and long division; and by the age of six he had moved on to Shakespeare and poetry, which he quoted at length. Later in life, Galton would use his own experience to propose a connection between genius and insanity, which forms the epigraph of this article. He suffered a severe nervous breakdown upon his father's death, causing him not to try for honours in mathematics and terminating his medical studies entirely.



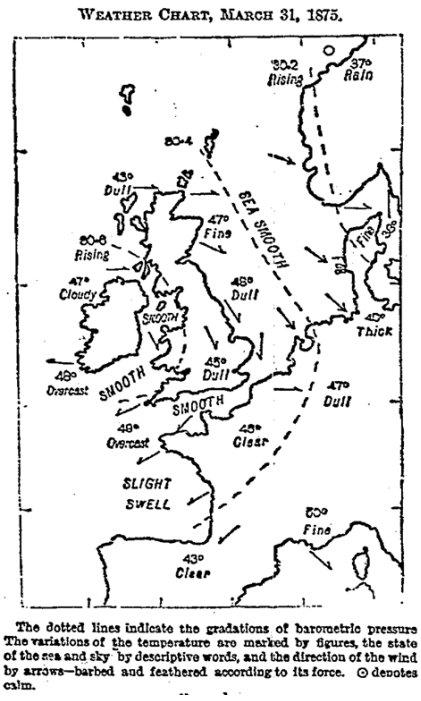
The Quincunx, as drawn by Francis Galton.

He had a predilection for counting or measuring, and was the first person to apply statistical methods to the study of human differences and the inheritance of intelligence, introducing the use of questionnaires and surveys for collecting data on human communities. His book, *Hereditary Genius*, was the first

social scientific attempt to study genius and greatness, particularly whether these traits could be inherited. It contained short biographies of eminent men followed by analyses concerning the eminence of their relatives, such as the former about Isaac Newton:

> *Newton, Sir Isaac; the most illustrious of English mathematicians and philosophers. Was exceedingly puny as a child; his life was then despaired of, but he grew to be strong and healthy. The three grand discoveries which form the glory of his life, were conceived in his mind before the completion of his twenty-fourth year: that is to say, the theories of gravitation, fluxions* [derivatives of continuous functions]*, and light.*[17]

He also founded psychometrics, the design of psychological tests to measure intelligence, aptitude, and personality. He contributed to meteorology as well, preparing the first weather map published in *The Times* (1 April 1875, showing weather from the previous day, 31 March), now a standard feature in newspapers worldwide. Galton would have rediscovered the Austrian monk and scientist Gregor Mendel's forgotten particulate theory of inheritance had he focused on discrete rather than continuous traits in his research. He also devised the classification system for fingerprints that survives to this day.



The very first weather map.

The publication of Darwin's *On the Origin of Species* in 1859 changed Galton's life in no small way. Henceforth, he devoted much of his life to exploring human variation and its implications, but in so doing invested his efforts in matters now considered far less noble, for he went on to found modern eugenics. It was he who coined that term as well as the phrase 'nature versus nurture' in its modern sense.[18] He was quite unhappy with the

[17] Francis Galton, *Hereditary Genius* (1892), 212.

[18] However, the terms had been contrasted previously, most notably by Shakespeare in *The Tempest*: 4.1. Galton's studies of twins led him to conclude that nature had the greater influence, laying the foundations for notions of inherent Aryan superiority espoused in the twentieth century with devastating consequences.

late marriages of eminent people and their few children, advocating incentives for these couples to have more children earlier.[19]

His less benign ideas reared their head in a controversial letter to *The Times* titled 'Africa for the Chinese', where he argued that the Chinese should be encouraged to immigrate to Africa and displace the supposedly inferior natives. This is because he viewed the Chinese as a race capable of high civilization only temporarily stunted by the recent failures of Chinese dynasties. In this letter, he also explained why Arabs or Hindoos (Indians) just would not suffice:

> *The Hindoo cannot fulfil the required conditions nearly as well as the Chinaman, for he is inferior to him in strength, industry, aptitude for saving, business habits, and prolific power. The Arab is little more than an eater up of other men's produce; he is a destroyer rather than a creator, and he is unprolific.*[20]

Godfrey Harold 'G H' Hardy (1877 – 1947)

A prominent English mathematician known for his achievements in number theory and mathematical analysis, Hardy is usually known by those outside mathematics for his essay on the aesthetics of mathematics, *A Mathematician's Apology*, which is considered to provide one of the best insights into the mind of a mathematician written for the layman.

He was extremely shy as a child, and was unsociable, distant, and eccentric throughout his life. He wrote numbers up to millions when he was just two years old and he amused himself in church by factorising the numbers of the hymns. Topping his class in most subjects during his school

[19] It was his protégé, Karl Pearson, known as the founder of mathematical statistics, who took up Galton's dangerous ideas far more aggressively, openly advocating war against races he deemed to be inferior.

[20] Francis Galton, letter to the Editor of *The Times*, June 5 1873.

years, Hardy won many prizes and awards but despised having to receive them in front of the entire school. He felt uncomfortable being introduced to new people and could not bear to look at his own reflection in a mirror to such an extent that, when staying in hotels, he would cover all the mirrors with towels.

He preferred his work to be considered pure mathematics because he abhorred war and the military uses of some applied mathematics. He went so far as to claim:

> *I have never done anything 'useful'. No discovery of mine has made, or is likely to make, directly or indirectly, for good or ill, the least difference to the amenity of the world.*[21]

Although Hardy wanted his mathematics to be 'pure' and devoid of any application, much of his work has eventually found applications in other branches of science. An avid cricketer, Hardy often played with the geneticist Reginald Punnett (after whom the Punnett square is named), who introduced a problem concerning Mendelian genetics to him in 1908. This led to Hardy's formulation of what is now known as the Hardy-Weinberg principle, and Hardy thus became an unwitting founder of a branch of applied mathematics.[22]

Yet when Hardy was asked by the Hungarian mathematician Paul Erdös[23] what his greatest contribution to mathematics was, he unhesitatingly replied that it was his discovery and mentoring of the Indian mathematician Srinivasa Ramanujan, whose extraordinary yet untutored brilliance Hardy almost immediately recognised. He called their collaboration, a relationship that has become celebrated in the history of mathematics, 'the one romantic incident in my life.'[24]

[21] GRO Register of Deaths: DEC 1947 4a 204 Cambridge – Godfrey H. Hardy, aged 70.

[22] The principle was actually known as Hardy's law in the English-speaking world until 1943, when the German-American geneticist Curt Stern pointed out that it had first been formulated independently in 1908 by the German physician Wilhelm Weinberg, who was largely ignored.

[23] Erdös has published more papers than any other mathematician in history, albeit with hundreds of collaborators.

[24] To understand Hardy's view of romance, it ought to be noted that apart from close friendships, Hardy had only a few non-physical relationships with similarly-minded young men. A life-long bachelor, he was cared for by his sister in the final years of his life.

Hardy also used the Riemann hypothesis[25] as an unusual form of insurance whenever he crossed the North Sea after a summer visit to his friend, the Danish mathematician and footballer Harald Bohr, brother of the Nobel Prize-winning physicist Niels Bohr.[26] Before leaving port, Hardy would send Harald a postcard with the claim that he had just proved the hypothesis. He reasoned that if the boat sank, he would have the posthumous honour of having solved the great problem; on the other hand, if God did exist (Hardy was an atheist), he would not let Hardy have that honour and would thus prevent the boat from sinking.

Among Hardy's many aphorisms, he once told the British philosopher Bertrand Russell:

> *If I could prove by logic that you would die in five minutes, I should be sorry you were going to die, but my sorrow would be very much mitigated by pleasure in the proof.*[27]

Kurt Gödel (1906 – 1978)

An Austrian logician, mathematician, and philosopher best known for his incompleteness theorems that ended the years of attempts to find a set of axioms sufficient for all mathematics, Gödel implied that not all mathematical equations are computable. The same could be said about his own life.[28]

In his family, he was called *Herr Warum*[29] because of his insatiable curiosity. At the age of six or seven Kurt suffered from rheumatic fever; he completely recovered, but for the rest of his life he remained convinced that his

[25]The Riemann hypothesis is part of Problem 8, along with the Goldbach conjecture, in David Hilbert's famous list of 23 unsolved problems. Hilbert said of his eighth problem: 'If I were to awaken after having slept for five hundred years, my first question would be: Has the Riemann hypothesis been proven?' It is also one of the Millenium Prize Problems for which the Clay Mathematics Institute offers a prize of a million dollars for a correct solution to any of the problems.

[26]Not only did Harald found the field of almost periodic functions, but he also won a silver medal at the 1908 Summer Olympic Games as a major goalscorer for the Danish national football team. Niels was also a passionate footballer, usually playing as goalkeeper; however, he did not play for the national team. Harald's popularity as a footballer was such that when he defended his doctoral thesis, the audience allegedly had more football fans than mathematicians.

[27]Russell happily agreed with Hardy about the delight of such a proof.

[28]See Paradox Issue 1, 2010, for a review of *Incompleteness*, a play about Gödel that explores this notion (ed).

[29]German for 'Mr Why'.

heart had suffered permanent damage. Later working as an unpaid lecturer in Vienna, he experienced a severe nervous crisis when a Nazi student assassinated Moritz Schlick, a philosopher whose seminar had aroused his interest in logic.[30] Spending several months in a sanitarium for nervous system disorders, Gödel became extremely paranoid at the age of 30, especially of being poisoned.

He eventually relocated to Princeton University once the Second World War commenced, where he met Albert Einstein. The two became close friends to the extent that they would take long walks together to and from the Institute for Advanced Study at Princeton University at which both worked. The nature of their conversations was a mystery to the other Institute members and towards the end of his life, Einstein confided to the economist Oskar Morgenstern (who helped found game theory) that his:

> *own work no longer meant much, that he came to the Institute merely... to have the privilege of walking home with Gödel.*[31]

Said by the physicist Freeman Dyson to be 'the only one who walked and talked on equal terms with Einstein,'[32] Gödel came up with paradoxical solutions to Einstein's field equations in general relativity as a present for his 70th birthday, with 'rotating universes' that would allow time travel, causing Einstein to have doubts about his own theory. Gödel also rejected Einstein's notion that God was impersonal. He believed firmly in an afterlife, stating in his own way:

> *I am convinced of the afterlife, independent of theology. If the world is rationally constructed, there must be an afterlife.*[33]

[30] Neither Schlick nor Gödel were Jewish; the precise motivations for the former's assassination are unclear.

[31] Rebecca Goldstein, *Incompleteness: The Proof and Paradox of Kurt Gödel (Great Discoveries) (2005)*.

[32] Freeman, Dyson, *From Eros to Gaia* (1993), 161.

[33] Philip J Davis, 'A Brief Look at Mathematics and Theology', *Humanistic Mathematics Journal* (2002) 26, 22.

Before going to his US citizenship exam with Einstein and Morgenstern, who had coached him since they were concerned about his unpredictable behaviour, Gödel claimed to have found a logical inconsistency in the US Constitution that would allow the US to become a dictatorship. When the Nazi regime was briefly mentioned in the exam, Gödel informed the presiding judge about his discovery, but neither the judge, nor Einstein or Morgenstern allowed him to finish his line of thought and he was awarded citizenship.

Gödel's mental instability and illness continued into later life. He took ghosts quite seriously and was quite convinced that the refrigerator and radiators in his various apartments in Princeton were giving off noxious gases. His obsessive fear of being poisoned reduced him to only eating food that his wife, Adele, prepared for him.

Unfortunately, she was hospitalised for six months and could no longer prepare his food. In her absence, he simply refused to eat, eventually starving to death. At death, he weighed only approximately 30 kg and his death certificate reported that he died of 'malnutrition and inanition caused by personality disturbance'.[34]

P versus NP: The universal panacea?

Imagine, if you will, The Last Computer Program You'll Ever Need. This little beast is capable of solving any problem you would want the answer to. Need it to sort out your timetable with zero clashes? The Program can do that for you. Piece of cake. Want it to solve your maths homework? Heck, feed The Program the Riemann Hypothesis and it'll solve it, write out a proof/disproof for you and adjust the margin sizes so that the paragraphs look perfect.

But be careful what you wish for – that which makes your job easy quickly makes your job redundant. The mathematicians will be the first to go. Then the engineers, the biochemists, the financial analysts and the operations managers. And once they've fallen, it's only a matter of time until the musicians and the Paradox writers do too. Why pay a hundred dollars an hour for human creativity when The Program can do that for free?

[34]Frederick Toates, Olga Coschug-Toates, *Obsessive Compulsive Disorder: Practical Tried-and-Tested Strategies to Overcome OCD* (2002), 221.

It may sound ridiculous, but we'd be more than halfway to writing such a Program if we discovered $P = NP$ – and we could probably give up on it altogether if $P \neq NP$. That's one reason why the P versus NP problem is such a big deal for mathematicians and computer scientists.[1]

In August 2010, Vinay Deolalikar, a researcher at HP Labs, announced that he had proved $P \neq NP$. Deolalikar is certainly not the first to claim to have solved P versus NP, but his paper is certainly the most credible in recent memory, and it gives us an excellent excuse to dive headfirst into the whole P versus NP issue.

Decision problems, *P* and *NP*

Computer scientists talk about *decision problems*, which are really just classes of yes-or-no questions like 'Could I still get to class on time if I could only use set L of paths?' (If you prefer, decision problems are Boolean functions on bitstrings, ie mappings from $\mathbb{Z}_2[X] \to \mathbb{Z}_2$.)

A problem can be solved by following a series of steps called an *algorithm*: think of algorithms as an abstraction of computer programs. There may be multiple algorithms to solve a particular problem, with varying strengths and weaknesses.

If you have an algorithm that correctly answers decision problems, you can efficiently use it to answer more complicated questions like '*How* do I get to class on time?' You do this in much the same way you would use yes-or-no questions like 'Is the secret integer greater than x?' to solve the more complicated 'What is the secret integer?'.

The other key idea in P versus NP is that of *polynomial time*. Roughly speaking, an algorithm runs in polynomial time if there exists some polynomial which *overestimates* the running time for any given input size. (Think of the $\gg$ symbol from first-year calculus.) Following from this:

> **Definition.** P is the set of all decision problems with polynomial-time algorithms.

[1] A useful introduction to P and NP, part of a larger series of lecture notes, can be found at: http://www.scottaaronson.com/democritus/lec6.html.

Think of P as the set of all problems we can solve efficiently.

Why did we choose polynomials instead of some other function type? Firstly, polynomials give a number of properties which simplify our analysis. We can chain programs in P one after another to get another program in P (closure under addition), run one as a subroutine within another (closure under multiplication), and avoid disputes about what units we use to measure time (ie closure under scalar multiplication).

Secondly, we choose polynomials since this boundary line reflects the difficulties computer scientists face in practice. To quote Scott Aaronson, an Associate Professor at MIT, 'Of the big problems solvable in polynomial time – matching, linear programming, primality testing, etc – most of them really do have practical algorithms. And of the big problems that we think take exponential time…most of them really don't have practical algorithms.' If we start discovering a lot of practical algorithms with $n^{\ln \ln n}$ running times, we may then have to rethink our boundary lines.

Here is an example of a problem in P:

> **Problem.** [SOCIAL BUTTERFLY] Input is a list of pairs of people who are friends. Is there a person with at least x friends?

A simple algorithm for solving this is to read in all the pairs of friends, keep tally of how many friends each person has, then answer 'yes' if and only if you spot someone with x or more friends. The time this takes is roughly proportional to the input size – we can call this a *linear-time*, hence polynomial-time, algorithm.

Here is an example of a problem believed not to be in P:

> **Problem.** [CLIQUE] Input is a list of pairs of people who are friends. Is there a group of x people who are all friends with each other?

While no polynomial-time algorithm is known for solving CLIQUE, it admits what we call polynomial-time *verification*. That means if the answer to a problem instance was 'yes', then we wouldn't need a correct algorithm to be convinced of this – a list of x people who were all friends with one another would

suffice. (Defining verification formally is a little hazy, but a good start would be having a polynomial-time verifier that checked justifications and never gave false positives.) From this we have our next definition:

> **Definition.** NP is the set of all decision problems such that 'yes' answers can be verified in polynomial time.

Think of NP as the set of all problems we can check the answers to quickly. Alternately, it is the set of all problems asking about the *existence* of some small object.

It is not difficult to show that $P \subseteq NP$. If you can solve a problem in polynomial time, you can convince me just as quickly by showing me your working. Lazier still, you could tell me to solve it myself.

The question 'Does $P = NP$?' asks 'If you can check answers to a problem quickly, can you find those answers quickly?'

A positive answer to this question would undoubtedly have non-trivial consequences on the way we handle and analyse information. Philosophically speaking, most problems that interest us in the real world are *those we can understand the answers to*. Here are just a few NP decision problems we wouldn't mind fast algorithms for:

- Can you build a structure (bridge, office building) satisfying design and safety requirements S and costing less than n million dollars?
- Can you pack the set of items X into k suitcases?
- Can you prove theorem T from first principles within l lines?

P versus *NP*: down the rabbit hole

There are a *lot* of problems in NP, and you might wonder how significant a $P \neq NP$ result really would be. After all, even if some problems in NP are too hard to solve in polynomial time, those problems might just be strange mathematical constructions we can't really understand. Mightn't we still find polynomial time algorithms for all the NP problems we care about?

As it turns out, we can't escape the P versus NP issue that easily. Most of the difficult problems we care about are inextricably tied to P versus NP.

Consider the following artificial problem:

> **Problem.** [NP-SOLVE] Input is a polynomial time verifier V (and, implicitly, its input). Is there a polynomial size justification the verifier will accept?

This problem is so general that it captures all of NP. From our definitions, any problem in NP must have a corresponding verifier V. So if we somehow wrote an efficient program to solve NP-SOLVE, then for any other problem $f \in NP$ we could just throw its verifier and input to that program and get our answer out, with only polynomial time spent transforming the problem from f language to NP-SOLVE language. We call NP-SOLVE an $NP - complete$ problem, because in this sense it is the *hardest problem in NP*.

> **Definition.** NPC is the set of all decision problems c such that:
>
> (1) $c \in NP$; and
> (2) a problem instance of any $f \in NP$ can be transformed into a problem instance of c in polynomial time.

The interesting part is that many less-contrived problems are in NPC. For example, CLIQUE, which we saw earlier, is NP-complete: if we have a fast way of solving CLIQUE, then there is a sneaky way of setting up CLIQUE-style problems which actually encode completely different problems in NP. Another classic example is SATISFIABILITY (SAT), which asks whether there is a set of yes-or-no variables satisfying a list of logical statements.

> **Lemma.** $P = NP \Leftrightarrow NPC \subseteq P$
>
> **Proof.** ($\Rightarrow$): follows from $NPC \subseteq NP$.
> ($\Leftarrow$): assume any NP-complete problem is in P. Then given any other NP problem we can solve it in polynomial time using a transformation (from NPC definition) into the first problem.

The above lemma naturally extends our idea of the NP-complete problems being the 'hardest problems in NP': a single polynomial algorithm for one

NP-complete algorithm would solve the lot and prove $P = NP$, and a single separation result would prove $P \neq NP$.

* * *

Most mathematicians and computer scientists closely involved with P versus NP believe that the answer is inequality.

Some of the major progress towards solving the question has been in determining what approaches *don't* work.[2]

For example, consider the concept of *oracle machines*. Like the Greek oracles of old, these oracles give us access to absolute truth, answering certain decisions so that our programs don't have to. For example, an oracle might instantly answer questions like 'Is n a prime?', 'Is X a true statement about the natural numbers?', or 'Does program P run forever?'.
(Students of logic may know that the last two questions are about as close to impossible-to-humanly-answer as one can get.)

In 1975 Baker, Gill, and Solovay described two kinds of oracle, which, if attached to a computer, would make $P = NP$ and $P \neq NP$ respectively. This means that there cannot be *relativizable* proofs regarding P versus NP (ie there cannot be a proof whose argument is indifferent to the presence of an oracle). This rules out techniques such as diagonalisation arguments.

In 1994, Razborov and Rudich proved a surprising result about proof strategies for inequality. In their paper they defined the idea of a *natural proof*, one that exploits properties that only some decision problems have. This includes what they call a 'commonly envisioned proof strategy' for $P \neq NP$: Formulate some 'difficulty' scoring function that operates on decision problems, inductively show that problems in P must have low 'difficulty', and show that some problem in NP has high 'difficulty'. Razborov and Rudich's result was this: under some widely-believed assumptions about random numbers, *natural proofs are self-defeating* – any attempt to prove $P \neq NP$ in this manner would inadvertently give an algorithm showing *equality* instead.

In 2009, Aaronson and Wigderson extended the concept of relativisation to a more general transformation called *algebraisation*, and demonstrated that any proof separating P from NP requires non-algebrising techniques – as well as

[2] An extensive list of P versus NP proofs over the years, both for equality and inequality, can be found at: http://www.win.tue.nl/∼gwoegi/P-versus-NP.htm.

the fact that, to date, no known separation result has used such techniques.

Following these results, inequality provers know that a separation result will require jumping through some serious hoops. If somebody wants to prove $P \neq NP$, they need to come up with something truly novel.

Deolalikar's inequality proof [3]

Given the sheer quantity of attempts to solve P versus NP – and why not? It's a Millenium Prize problem, which means $\$1\,000\,000$USD from the Clay Mathematics Institute to whoever solves it – it takes something special to get the experts to sit up and take notice. Vinay Deolalikar's proof from August 2010 is certainly that. It combines ideas from mathematical logic, statistical physics and other domains.[4]

Imagine taking a trivially easy instance of SAT (eg 'Is there any set of n variables satisfying an empty set of constraints?') and adding constraints to it one by one from a uniform random distribution. Initially, when there are few constraints, the probability of there being a solution and the expected number of solutions is high. After many constraints are added these expectations decrease towards zero. Between these two points the system undergoes property transitions with names like 'clustering', 'freezing' and 'condensing'.

Empirically, problem instances from near the freezing transition are the ones which are most computationally difficult to solve in practice.

Deolalikar appears to argue that the phase transition for SAT endows it with properties that forbid the existence of a polynomial time algorithm (using certain properties of polynomial time algorithms that arise when modelled in first-order logic). Being a proof by contradiction, it may evade the natural proof barrier that plagues similar attempts to establish complexity measures.

At first blush, the proof seemed credible, and paved the way for an immense discussion on the Internet drawing in experts from all corners of mathematics

[3] **Obligatory disclaimer**: the author may have completely mangled his description of the specific mathematical apparatus used by Deolalikar, particularly the psuedo statistical mechanics. Readers after the hard mathematical truth are advised to read arcane computational complexity journals instead of Paradox, and to go outside every once in a while.

[4] Much of the discussion regarding Deolalikar's proof can be found on Dick Lipton's blog and on Michael Nielsen's polymath wiki: http://tinyurl.com/lipton-pnp; http://tinyurl.com/nielsen-pnp.

and theoretical computer science. It was a flurry of activity that *New Scientist* was quick to tout as 'a new way of doing mathematics…blogs and wikis rivalling blackboards and journals'.

Among the major contributors to the debate was Australian Fields medallist Terence Tao, who helped to point out several potential areas of weakness in the proof. For instance, one of the characterisations of P as a logical grammar does not appear appropriate for the arguments later used in the paper.

Summarising after half a week of intense discussion, Tao wrote:

> *Does Deolalikar's proof, after major changes, give a proof that $P \neq NP$?…The best answer [to this] we currently have is 'Probably not, unless substantial new ideas are added.'*

Others are more optimistic. Dick Lipton writes:

> *I hesitate to make parallels, but recall that Andrew Wiles's first proof fell apart. He needed the help of Richard Taylor and another year to get his final wonderful proof of Fermat's Theorem.*

The proof itself has been removed from Deolalikar's web site. In its place is a short paragraph:

> *The preliminary version was meant to solicit feedback from a few researchers as is customarily done…I have fixed all the issues that were raised about the preliminary version in a revised manuscript; clarified some concepts; and obtained simpler proofs of several claims. Once I hear back from the journal as part of due process, I will put up the final version on this website.*

Deolalikar is not the first person to claim to have solved P versus NP, and he won't be the last either. In the time it took me to write this article, a fresh equality proof appeared on the blogosphere, this time from Vladimir State University. Like all attempts on this problem it's at least worth perusing, but I wouldn't hold my breath…

Solutions to Problems from Last Edition

We had a number of correct solutions to the problems from last issue. Below are the prize winners. The prize money may be collected from the MUMS room (G24) in the Richard Berry Building.

Charlotte Lau solved problem 2 and may collect $3.
Raj Rahya solved problem 5 and may collect $3.
Lau Cheuk Yin solved problem 7 and may collect $5.

1. How many terms in the arithmetic sequence $8, 21, 34, ...$ consist solely of the digit 9?

   Solution: We consider the problem modulo 13, since the sequence consists of all positive integers congruent to 8 mod 13. First, we note that 99 lies in the sequence, since $99 = 13 \times 7 + 8$. Moreover, since 13 is prime, from Fermat's Little Theorem we know that $10^{12} \equiv 1$ (mod 13). Therefore, for any positive integer k, $10^{12k+2} - 1 \equiv (10^{12})^k \times 10^2 - 1 \equiv 1^k \times 10^2 - 1 \equiv 99 \equiv 8$ (mod 13). Thus, any number consisting of $12k + 2$ consecutive 9s will lie in the sequence.

2. Prove that for any $n \geq 6$, an equilateral triangle can be dissected into n smaller equilateral triangles.

   Solution (thanks to Charlotte Lau): First we notice that an equilateral triangle can be divided into 4, 6 and 8 sub-equilateral triangles, by using one triangle of side-length $\frac{1}{2}$, $\frac{2}{3}$ and $\frac{3}{4}$ respectively, and by tiling the remaining *strip* with 3, 5 and 7 triangles of side-length $\frac{1}{2}$, $\frac{1}{3}$ and $\frac{1}{4}$ respectively, alternating up and down. From this, it is clear that if an equilateral triangle can be divided into n sub-equilateral triangles, then it can also be divided into $n-1+4 = n+3$, $n-1+6 = n+5$ and $n-1+6 = n+5$ sub-equilateral triangles, by sub-dividing further one of the sub-triangles for 4, 6 or 8 sub-sub-triangles respectively.

   It then suffices to prove that for each integer $n \geq 6$, there is a solution in the non-negative integers for $1 + 3i + 5j + 7k = n$. This is equivalent to showing that there are non-negative integer solutions to $3i + 5j + 7k = n$ for all $n \geq 5$. We divide into three cases: for $n = 3c$, we take $(i, j, k) = (c, 0, 0)$; for $n = 3c + 1$ we take $(i, j, k) = (c - 2, 0, 1)$ (since we know $c \geq 2$); for $n = 3c + 2$ we take $(i, j, k) = (c - 1, 1, 0)$ (since we know $c \geq 1$).

3. Find all positive integers n such that $2^{200} + 2^4 + 2^n - 2^{103}$ is a perfect square.

   Solution: First, we notice that the expression can be written as $(2^{100} - 2^2)^2 + 2^n$. If we suppose that this equals some perfect square x^2, then we can rewrite and factorise as $2^n = x^2 - (2^{100} - 2^2)^2 = (x - 2^{100} + 2^2)(x + 2^{100} - 2^2)$. Since both the bracketed expression are integers, we have $x - 2^{100} + 2^2 = 2^a$ and $x + 2^{100} - 2^2 = 2^b$ for some $a + b = n$. Subtracting the first equation from the second yields: $2^b - 2^a = 2 \times 2^{100} - 2 \times 2^2$ or $2^a(2^{b-a} - 1) = 2^3(2^{98} - 1)$. Equating odd and even factors of each expression, we must have $a = 3$ and $b - a = 98$, so $n = a + b = 3 + 101 = 104$ is the only solution.

4. Does there exist an $n > 1$ such that the integers from 1 to n^2 can be arranged in an nxn grid so that the products of the integers in every row and column is constant?

   Solution: No. Bertrand's Postulate states that, for any integer $k > 1$, there exists a prime p such that $k < p < 2k$. For any $n > 1$, if we choose $k = \frac{n^2}{2}$ if n is even and $k = \frac{n^2+1}{2}$ if n is odd, we know from Bertrand's Postulate that a prime p exists such that $\frac{n^2}{2} < p \leq n^2$. Now, clearly $2p > n^2$, so precisely one factor of p lies in the set $1, 2, ..., n^2$. Thus, the products of the integers in the row and column containing this factor cannot possible equal the products of the other rows and columns.

5. How many 'valid' position-pairs of the hour and minute hand on a 12-hour analogue clock (ie. positions that are possible given the motion of these hands over time) are equally 'valid' if the hands switch places?

   Solution: If we let $360 > h \geq 0$ and $360 > m \geq 0$ be the positions of the hour and minute hands respectively in degrees measured clockwise from 12 o'clock, once we realise that the minute hand moves 12 times as fast as the hour hand, we get that any 'valid' time satisfies $m = 12h - 360a$ for some integer a, and conversely any pair (h, m) satisfying this relation represents a valid time (being $\frac{h}{30}$ hours after 12 o'clock). If the time is still 'valid' after switching the hands, then $h = 12m - 360b$ for some integer b. We need a pair (h, m) satisfying both these relations. Substituting the first relation into the second, we get that $h = 12(12h - 360a) - 360b = 144h - 360c$ for some new integer c. Thus $143h = 360c$ or $h = \frac{360c}{143}$. This equation has 143 solutions in the range $0 \leq h < 360$, each of which provides a solution pair (h, m) satisfying both relations.

6. A 5x5 array contains all 1s or 0s. A *move* consists of toggling an nxn grouping of squares in the array (the grouping must lie fully within the array), where n can be 2, 3, 4 or 5. The array originally contains 24 0s and a solitary 1. For which starting positions of the 1 can the grid be modified to contain all 0s?

   Solution: We will use the following notion: an (a, b, c) *move* consists of a toggling an axa sub-array with bottom-left corner located at square (b, c). First, an array with a 1 located in the centre can be cleared of 1s by using the following five *moves*: (3,1,1), (3,3,3), (2,1,4), (2,4,1) and (5,1,1). Second, an array with a 1 elsewhere cannot be cleared. To see this, consider S to be equal to the sum of all the digits in the array modulo 2. To begin with $S = 1$ and to end $S = 0$. Now, notice than any toggle with a even keeps S constant, whereas every toggle with a odd increases S by exactly 1 (mod 2). Thus, to change S from 1 to 0, we must use an odd number of odd-sized toggles. However, each odd-sized toggle will necessarily toggle the centre square of the array, so any sequences of *moves* changing S from 1 to 0 must toggle the centre square an odd number of times. Thus, it must effect a *net* toggle on the centre square. The centre square therefore contains the solitary 1.

7. Find all solutions in positive integers to the following system of equations: (1) $a + b + c + d = 12$; (2) $abcd = 27 + ab + ac + ad + bc + bd + cd$.

   Solution (thanks to Lau Cheuk Yin): First, by the AM-GM inequality, $\frac{ab+ac+ad+bc+bd+cd}{6} \geq \sqrt[6]{ab \times ac \times ad \times bc \times bd \times cd} = \sqrt[6]{(abcd)^3} = \sqrt{abcd}$, with equality if and only if $ab = ac = ad = bc = bd = cd$ or $a = b = c = d = 3$. As $abcd = 27 + ab + ac + ad + bc + bd + cd$, we have $abcd - 6\sqrt{abcd} - 27 \geq 0 \Rightarrow (\sqrt{abcd} - 9)(\sqrt{abcd} + 3) \geq 0 \Rightarrow \sqrt{abcd} \geq 9$ (since $\sqrt{abcd} > 0$). On the other hand, again by the AM-GM, $\frac{a+b+c+d}{4} \geq \sqrt[4]{abcd} \Rightarrow 3 \geq \sqrt[4]{abcd} \Rightarrow 9 \geq \sqrt{abcd}$. So $9 \leq \sqrt{abcd} \leq 9 \Rightarrow \sqrt{abcd} = 9 \Rightarrow abcd = 81$, with equality if and only if $a = b = c = d = 3$. Thus, the only solution to the system is $(a, b, c, d) = (3, 3, 3, 3)$.

Solution to puzzles from page 6:
Puzzle 7: Let m and s be the ages of mother and son. The first piece of information yields $m = s + 21$, while the second yields $m+6 = 5\times(s+6)$. Solving these simultaneously, we get $m = 20 + \frac{3}{4}$ and $s = -\frac{3}{4}$. Since the son is thus 9 months away from being born, his father is (presumably) currently conceiving him!

Paradox **Problems**

Below are some puzzles and problems for which cash prizes are awarded. Anyone who submits a clear and elegant solution may claim the indicated amount (up to a maximum of four per person). Either email the solution to the editor (see inside front cover for address) or drop a hard copy into the MUMS room (G24) in the Richard Berry Building; please include your name.

1. (\$2) Two players take turns placing coins, of radius 1, onto an mxn table, such that no two touch. The first player unable to place loses. For which m and n does the first player have a winning strategy?
2. (\$3) Prove that each 4x7 grid coloured black and white at random contains a rectangle such that each (distinct) corner square is of the same colour. Prove this is not true of a 4x6 grid.
3. (\$3) 15 people, each holding a ball, stand in a field. Each passes their ball to the person nearest them; no two distances are equal. Prove that: (1) there is someone without a ball; and (2) no-one has more than 5 balls.
4. (\$3) A square piece of paper is progressively cut up into smaller pieces by, at each step, taking one piece and cutting it into two by a straight cut. What is the minimum number of cuts needed to get a hundred (non-regular) octagons?
5. (\$3) For any convex polyhedron with an even number of edges, prove it is possible to attach an arrow to each edge such that each vertex of the polyhedron has an even number of arrows directed towards it.
6. (\$4) Which positive integers cannot be represented as $\frac{a}{b} + \frac{a+1}{b+1}$, with a and b positive integers?
7. (\$5) $2n$ people sit around a table with k chocolates distributed among them. A person may give a chocolate to their neighbour, but only after eating first one themselves. Nominating a *head* of the table, what is the minimum k such that, irrespective of the initial distribution of the lollies, there is a way for the *head* to get a chocolate? What is the minimum k such that *everyone* can get a chocolate?

Paradox would like to thank Christopher Chen, Sam Chow, John Dethridge and Michael Phillips for their contributions to this issue.