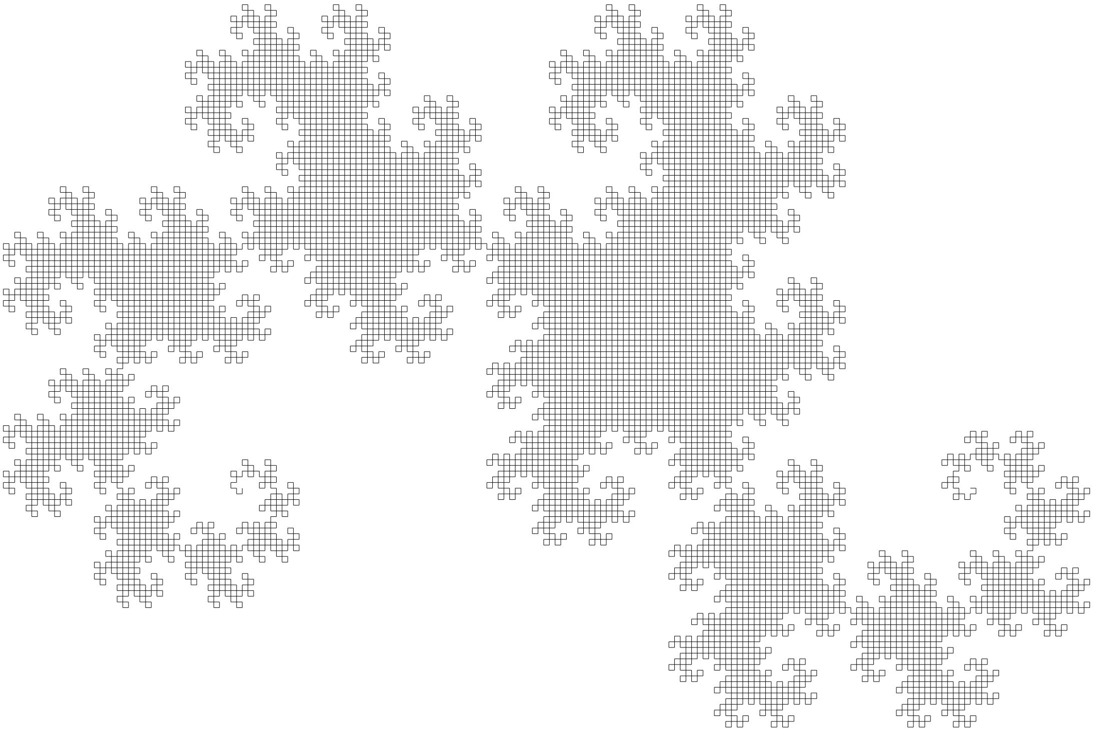
The Invariant

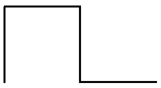


Issue 15

The Invariant

Oxford University Invariant Society

The cover illustration is a fractal known as a 'dragon curve', generated by replacing all the lines in this diagram with itself.



It has a connection with the cover of Issue 14 in that first-year undergraduates in computation draw both patterns in one of their practicals. This version was produced by a short PostScript program written by Ian Collier.

Contents

Editorial

Regrettably, it has been some time since the last issue of *The Invariant* was published, but at last here is another. On this occasion, however, the delay is not entirely the fault of the Editor: until September 1995 only two articles had been submitted for publication. Looking back through editorials of previous magazines shows that this is not an unusual situation. I therefore sincerely urge readers to think *now* about material for the next issue! Almost anything related to the Invariant Society will be accepted, for example:

- Articles exploring some aspect of mathematics
- Mathematical puzzles
- Reports of previous Invariants meetings
- Letters to the editor.

Items will be accepted on paper or by email; items sent electronically may be in plain ASCII or in $\TeX$/$\LaTeX$. Any member of the committee should be able to tell you who the current Editor is and how to contact him or her.

Anyway, now that we have a magazine, you will find a wide variety of articles within, so I hope that you will find something to interest you—whether you are looking for serious mathematics or you just want a bit of fun. As usual, my job as Editor is to showcase the works of the individual authors while preserving some degree of uniformity in style and eliminating the most obvious mistakes. Credit should go to the authors for their work and ideas, but if there are any mistakes then blame should go to the Editor.

Before you read further, you may like to try out the puzzle which is the subject of the article entitled 'Prime Suspect' and is as follows. There are two integers between 3 and 98 inclusive. Mr. S has been told their sum and Mr. P their product. The following truthful conversation occurs.

P: I don't know the two numbers.
S: I knew you didn't. Neither do I.
P: Now I know them!
S: Now I do, too!

What are the two numbers?

Ian Collier.

Pin the finite subcover on the compact topological space

(A beginner's guide to mathematical party games)

Juliette White

worc0026@sable.ox.ac.uk

Since the days when Gauss' schoolchums entertained themselves by playing "Let's see how long a rest Carl will give our teacher this time", the mathematical party game has evolved to its current highly sophisticated form. To prove that mathematicians know exactly how to have a good time, I present here a survey of some of my favourite variations and attempt to blame Catherine Jackson for any particularly fiendish aspects of these.

Mathematical "Just a Minute"

In each round, a nominated player must speak for a minute on a given subject without hesitation, deviation, repetition or evocation of the axiom of choice—or indeed making any mathematical howlers. Other players may challenge on any of these faults with a cry of "Eureka" and if the challenge is declared valid continue to talk on the given subject instead. The person speaking at the conclusion of the minute is awarded a point. Suitable topics might be "My favourite lemma", "Invariants' scandals" or "The Euclidean plane". A warning should be issued that when I introduced this game at the 1994 Christmas party an ancient historian almost won.

Mathematical "Give us a clue"

Similar to the usual charades games but all the words are mathematical and the standard categories are replaced by the following.

- Great mathematician: Point at the society's president or other predesignated person (who should be specifically chosen to be the person who will find this most embarrassing).
- Theorem: Hold up a finger as with a flash of inspiration—in memory of the delight of the mathematician who first proved the theorem.
- Conjecture: Adopt a puzzled expression.
- Term: Scribble on an imaginary note pad.
- Process or algorithm: Type numbers into an imaginary calculator.

There is a special rule forbidding the drawing of mathematical symbols in the air. Extra points may be awarded for correct guesses without the use of homonyms, but I don't think I'd have stood much chance of acting out "The Weierstrass M-test" without them...

Mathematical "Call My Bluff"

Three possible definitions of an obscure mathematical term are read out by one team. The opposing team has to guess which definition is correct. For instance, possible definitions of "meagre" could be:

(a) A natural number is said to be meagre if any power of it can be written as the sum of two primes.
(b) A nilpotent group is said to be meagre if it is non-Abelian.
(c) A subset X of a metric space is said to be meagre if it is the union of a countable number of sets which are nowhere dense in X.

—the correct definition being (c). Of the games described here this is the one with the longest-known history, dating back to at least the 1960s and with documentation of intervarsity matches having been played.

Miscellaneous

Ideas stolen from other radio or television programmes may prove useful for mathematical party games. It should be pointed out that not all radio or television programmes can be so easily adapted. Imagine, for instance, a mathematical version of "Blankety-Blank" ("If we assume the function is blank, then we have the following result...") or Family Fortunes ("We asked one hundred mathematicians to tell us their favourite number"). Standard party games can prove inspirational too—mathematical Chinese whispers ("The central extension F/J is irreducible if and only if any maximal subgroup of F which contains JF' also contains K") or hangman. You could even play a version of musical statues where you have to try to freeze in a position resembling a mathematical symbol.

Topological party games

Aside from the classic game of Twister the following is a lovely illustration that the continuous image of a path-connected set is path-connected. With one person evicted from the room, everyone else holds hands in a circle and without letting go of each other's hands tries to tangle themselves up as much as physically possible. The evict returns to the room and tries to restore everyone to an untangled ring again, during which process hands must remain firmly clasped.

Countdown numbers game

How desperate are you? You could of course try the variation in which you are given various axioms and have to deduce a given theorem from these axioms. Godel's incompleteness theorems add some uncertainty to the proceedings.

Games involving logic to some degree

Coming dangerously close to real Mathematics for some maybe, but if people are too drunk to remember how to count in binary then you could try playing Nim's game.

If all this competitiveness is too demanding then you have no other option but to sit back and discuss whether or not Fermat's Last Theorem has in fact eventually been proved.

Prime Suspect

Gareth Leyshon[1] and Richard Green[2]

gjl@astronomy.cardiff.ac.uk, math0001@sable.ox.ac.uk

Editor's note: an email containing the following text was sent to Gareth, who spent six hours solving it with Richard. Gareth, a previous contributor to this magazine, wrote the solution up and donated it for publication.

> There are 2 integers n and m between 3 and 98 inclusive. Mr. S has been told their sum and Mr. P their product. The following truthful conversation occurs:
>
> P: I don't know n and m.
>
> S: I knew you didn't. Neither do I.
>
> P: Now I know them!
>
> S: Now I do, too!
>
> What are the values of n and m?
>
> P.S. I reckon you'll need a computer.

OK, let's make this sound mathematical. Let a *pair* be a set of two integers m and n such that $2 < m, n < 99$. Let us say that a pair whose product can be factorised into a different pair is *refactorisable* (we can also speak of their product as being a refactorisable product). To express a number as the sum of a pair is to *decompose* it.

The set of pairs is finite, and therefore so is the set of products; a little handle-turning could produce a list of refactorisable pairs (which we'll call set R). A computer could produce a complete list—but Richard and I didn't use that method. I'm not sure if that list would help you, anyway. Now, think about the problem...

Step One

Mr. P says "I don't know..."

Let's call the product $P = mn$, so P is a member of set R. That is, P is refactorisable.

Step Two

Mr. S says "I don't know"—so the sum, $S = m + n$, cannot be 6 or 7 or 195 or 196, because these sums would be uniquely decomposable.

Mr. S also says "I know Mr. P doesn't know". This means that *all* the decompositions of S must be refactorisable pairs. Let a number with the property that all decompositions are refactorisable pairs be called a *green* number, in recognition of my erstwhile colleague. The sum S is a green number.

[1] BA. (Keble), now Ph.D. student at Cardiff, Department of Physics and Astronomy
[2] BA. (Univ), Ph.D. (Warwick), now at the Mathematical Institute, Oxford

Now $7 < S < 195$. How many sums within this range have no non-refactorisable decompositions (that is, how many sums are green)? We shall work by a process of elimination, eliminating all values with *at least one* unique (that is, non-refactorisable) decomposition.

S must be less than 100. Since 97 is prime, $S > 99$ can be expressed as 97 plus some number between 3 and 98 inclusive. If this were the case, one of m and n might be 97, which gives a uniquely factorisable decomposition, and Mr. S couldn't be sure that P was refactorisable. This eliminates values up to $S = 97 + 98$, and we've already eliminated $S = 98 + 98$.

Similarly, S must be less than 56. Since 53 is the lowest prime greater than $98/2 = 49$, all S values between 56 and 100 can be decomposed as pairs containing 53, which are not refactorisable. So $7 < S < 56$.

Any even number can be expressed as a sum of two primes, so if S were even, Mr. S couldn't be sure m and n weren't both prime. Suppose S *is* even, and decompose it to a pair of primes. Since we have already restricted S below 98, both primes must be less than 98—and since $S = 4$ is not permitted, both primes must be odd, and so greater than or equal to 3. Both primes are therefore in the range 3–98 and are a valid, and uniquely factorisable, decomposition. Hence there are no even green numbers.

So S is odd, and must be the sum of an odd and an even. Because P is refactorisable, it must have at least three (not neccessarily distinct) prime factors, and because one of m and n is even, 2 must be a prime factor of P.

We can write a list of the remaining possible values of S, which will include every odd number between 9 and 55 inclusive. Are they all green? Let's now construct an algorithm to generate every possible decomposition of some S, and to refactorise the decomposition. If the algorithm fails for that S then that S is not green.

We know that we want an odd-even decomposition, which must be of the form $S = 2a + b$. Now $2a$ must be in the range 4 to $S - 3$ because of the limits on $2a$ and b. Can we always refactorise this to the pair $a, 2b$?

If $a = b$ and is prime then the refactorisation is not distinct. So no $S = 2a + a = 3a$ is green. All numbers of the form $3 \times$ *prime* can be struck off from our list of candidates.

If $2a = 4$ and b is prime, the pair is not refactorisable. So any S which can be expressed as $4 +$ *prime* is not green, and can be deleted from our list.

If b is non-prime (and $2a$ is still 4), it must have at least one prime factor no greater than its square root; since b is within the $2 < b < 99$ range, this prime factor is less than 10 and will multiply the 4 to a number no greater than 40—well within range. Since b is an odd nonprime, dividing out this prime factor must leave an odd remainder, hence the remainder is also greater than 2 and must be in range.

So if b is non-prime, we can then consider values of $2a$ between 6 and $S - 3$. For the possible values of S, a is always within range. Now $S < 57$ so $b = (S - 2a)$ is always less than 51. In fact, b, being odd, cannot exceed 49 and so $2b$ cannot exceed 98, and the refactorisation into $a, 2b$ is valid.

Hence the green numbers are all odd numbers between 7 and 55 inclusive which are not expressible as $3 \times$ *prime* or $4 +$ *prime*.

This list can easily be constructed. We can identify the whole set of green numbers: 13, 19, 25, 29, 31, 37, 43, 49, 53 and 55.

Let any pair of numbers whose sum is green be said to be a green pair (pairs have many-to-one mappings to both the set of green sums and the set of refactorisable products).

Step Three

Mr. P says "Now I know!" P is a refactorisable number only one of whose factorisations is a green pair.

If a green pair can be refactorised to give another green pair, let us say it is *bright* green. If it cannot, let it be *pale* green. P's factorisation is neccessarily pale green.

If a product is refactorisable, it could be classified as being *dark* (no green factorisations, all the factorisations—of which there must be at least two—being 'grey' pairs,[3] pale (exactly one green factorisation—a pale green pair—and at least one grey factorisation), or bright (more than one green factorisation, all into bright green pairs, plus an indeterminate—zero, one or more than one—number of grey factorisations). Non-refactorisable products have a unique factorisation which cannot be a green pair by the definition of greenness.

Step Four

Mr. S says "Now I know, too!" S is a green number only one of whose decompositions is pale.

Step Five

What are m and n?

It turns out that the solution to step four is unique. All but one of the green numbers are multiply pale, that is, they have at least two pale decompositions (I don't know enough set theory to know if this neccessarily follows from the above). So we can go through our list of green numbers and eliminate all those with at least two pale decompositions.

We could take each green candidate and construct possible decompositions methodically: $3, (S-3)$; $4, (S-4)$; $5, (S-5)$; ... and test every possible refactorisation of each pair for greenness. We must test *every possible refactorisation* of a decomposition to make sure none of them is green, so that the decomposition is pale, but it is sufficient to find *two* pale decompositions to eliminate each candidate.

By way of a shortcut, we could be clever about the decompositions which we test, by looking for prime numbers p.

- Test (a): If the green candidate can be expressed as $(p + 2^z)$ then p will be odd and $z > 2$ ($z = 1$ is below limits, and if $z = 2$ the pair could not be green). There will be at least one refactorisation, to $2p$ and 2^{z-1}, and more if $z > 3$. But any possible refactorisation would be an even-even pair. Since all green numbers are odd, such a pair cannot possibly be green.
- Test (b): If the green candidate can be expressed as $(6 + p)$, the only possible refactorisation is to $3, 2p$. If $p > 26$ then the sum of the refactorisation will be too large to be green. Otherwise the refactorisation must be tested by inspection.
- Test (c): If the green candidate can be expressed as $(18 + p)$, refactorisations to $3p, 6$ and $3, 6p$ cannot give green pairs as the sum would be divisible by 3—and it can be

[3] In environmental jargon, the opposite of green is grey.

seen by inspection that none of the green numbers is a multiple of 3. The only other refactorisation is $9, 2p$ which must be tested by inspection.

Let's analyse all the green numbers for multiple paleness using these tests. All the following numbers can be eliminated.

- $55 = 47 + 8$ (pale by test 'a') $= 32 + 23$ (pale by test 'a')
- $53 = 37 + 16$ (pale by test 'a') $= 6 + 47$ (pale by test 'b' since $47 > 26$)
- $49 = 32 + 17$ (pale by test 'a') $= 41 + 8$ (pale by test 'a')
- $43 = 32 + 11$ (pale by test 'a') $= 6 + 37$ (pale by test 'b' since $37 > 26$)
- $37 = 32 + 5$ (pale by test 'a') $= 29 + 8$ (pale by test 'a')
- $31 = 23 + 8$ (pale by test 'a') $= 18 + 13$ (pale by test 'c' since it refactors to $9, 26$ whose sum is 35, which is grey)
- $25 = 8 + 17$ (pale by test 'a') $= 18 + 7$ (pale by test 'c' as it refactors to $9, 14$ and 23 is grey)
- $19 = 16 + 3$ (pale by test 'a') $= 11 + 8$ (pale by test 'a')
- $13 = 8 + 5$ (pale by test 'a') $= 6 + 7$ (pale by test 'b' since it refactors to $3, 14$ and 17 is grey)

So these three tests are *sufficient* to prove the multiple paleness of all green numbers other than 29. They are not sufficient to show that 29 has only one pale decomposition. We must test all possible decompositions of 29 for green refactorisations.

Decomposition	Refactorisation	Sum	Green?
$3, 26$	$6, 13$	19	yes
$4, 25$	$20, 5$	25	yes
$5, 24$	$40, 3$	43	yes
$6, 23$	$46, 3$	49	yes
$7, 22$	$14, 11$	25	yes
$8, 21$	$24, 7$	31	yes
$9, 20$	$45, 4$	49	yes
$10, 19$	$38, 5$	43	yes
$11, 18$	$22, 9$	31	yes
$12, 17$	$51, 4$	55	yes
$13, 16$	(pale by test 'a' above)		
$14, 15$	$30, 7$	37	yes

Hence, alone among the green numbers, 29 has only one pale decomposition. The values of m and n are 13 and 16. Mr. P's product is 208. Mr. S's sum is 29. Problem solved.

Despite the hint that "you will probably need a computer", it was done in practice using only two neural networks running wetware and a calculator. The solution above (greatly refined by virtue of being understood now) can be understood without use even of a calculator.

Beating Carol at her own game

Jonathan Young

jonathan.young@merton.ox.ac.uk

The Problem

Given Z, a random integer between 101 and 999, and a multiset $X = \{x_1, x_2, x_3, x_4, x_5, x_6\}$ of random integers, find a value F, calculated from a subset of X using only the arithmetic operators of addition, subtraction, multiplication and division with zero remainder, such that $|Z-F|$ is minimised. Each element of X must be used at most once in the calculation of F. The multiset X will satisfy the following constraints for some parameter $k \leq 4$:

$$\{x_1, \ldots, x_k\} \subseteq \{25, 50, 75, 100\}$$
$$\{x_{k+1} \ldots, x_6\} \subseteq \{1, 1, 2, 2, \ldots, 10, 10\}.$$

For example, suppose $Z = 170$ and $X = \{50, 2, 3, 3, 6, 8\}$. Let:

$$\begin{array}{lllllll}
F_1 &=& x_1x_2 + x_4x_5 + x_2 &=& (50\cdot 3) + (3\cdot 6) + 2 &=& 170 \\
F_2 &=& (x_3x_4 + x_5)x_6 + x_1 &=& (3\cdot 3 + 6)8 + 50 &=& 170 \\
F_3 &=& (x_1 + x_5)x_4 + x_2 &=& (50 + 6)3 + 2 &=& 170 \\
F_4 &=& [(x_4 + x_5)x_3 + x_6 + x_1]x_2 &=& [(6 + 3)3 + 8 + 50]2 &=& 170 \\
F_5 &=& (x_1 - x_5)\left(\frac{x_6}{x_2}\right) - x_3 - x_4 &=& (50 - 6)\left(\frac{8}{2}\right) - 3 - 3 &=& 170.
\end{array}$$

Clearly, solutions for $|Z - F| = 0$ need not be unique. However, the existence of F such that $|Z - F| = 0$ is not guaranteed either, as is shown by the case $X = \{1, 1, 2, 2, 3, 3\}$ and $Z > 100$.

Solutions

Clearly, from the number of exact solutions the above problem is 'easy'. Reasons for this include the value $k = 1$ ('the standard problem'), a relatively low value of Z, a value of x_1 other than 75 (75-times table is tricky!) and a good 'spread' of numbers less than 10, including the nearest integer to $\frac{Z}{x_1} = \frac{170}{50}$, in this case 3.

The five examples above demonstrate the main strategies which give a good chance of a minimal value of $|Z - F|$ being found in a short time using mental arithmetic.

Case 1 uses the approximation $\frac{170}{50} \approx 3$ to simplify the problem, which loses flexibility but makes the calculation easier. In the example (F_1) the reduced problem is to solve for $\tilde{Z} = 20$ and $\tilde{X} = \{2, 3, 6, 8\}$, which is trivial since $20 = 6\cdot 3 + 2 = (8 + 2)\left(\frac{6}{3}\right) = 8\cdot 3 + 2 - 6 = 2\cdot 6 + 8$.

Finding $\tilde{F}$ such that $|\tilde{F} - \tilde{Z}| = 0$ implies that F can be found such that $|F - Z| = 0$, where the F is some obvious function of $\tilde{F}$.

Case 2 demonstrates a particularly useful technique for cases in which $Z < 200$, especially when x_1 is 75 or 100, or $k > 1$. For example, to solve $Z = 181$ and

$X = \{100, 75, 6, 2, \mathrm{x}, \mathrm{x}\}$, observe first that $181 = 100 + 75 + 6$ rather than observing that $\frac{181}{2}$ is approximately 75 or 100 and going through the procedure above.

Case 3 is useful when the nearest integer to $\frac{Z}{x_1}$ is a member of X—call it x_r—but the fractional part is rather large, as in this case since $\frac{170}{50} - 3 = 0.4$. Calculate instead $\left|\frac{Z}{x_r} - x_1\right|$. Then take the remaining member of X (say x_s) which is closest to this value and consider finding F' to solve for $Z' = Z - x_r(x_1 \pm x_s)$ and $X' = X - \{x_1, x_r, x_s\}$.

Here, $Z' = 170 - 3(50 + 6) = 2$ with $X' = \{2, 3, 8\}$.

Also, $Z' = 170 - 3(50 + 8) = 2 - 6$.

Case 4: this factorisation trap is one of the main reasons why many mathematicians are bad at this game. Generally speaking, attempting to find the factors of Z in terms of the members of X is time-consuming and often very inefficient at scoring points if no exact solution can be observed.

For instance, if $Z = 504$ and $x_i = 8$ then it is clever to see that it would be desirable to find $\frac{504}{8} = 63$ using the remaining 5 numbers. However if the best that can be done is 65, say, then the error $|Z - F|$ is 16, which does not score and these calculations will have wasted a great deal of time.

The best occasions to try this sort of approach are when you want to be ostentatious when a solution of the form of case 1 or 3 has already been spotted, or when all obvious attempts at using these case methods have failed and there is enough time remaining to try the divisibility rules, etc.

Case 5 is similar to case 3, but note the use of subtraction and division, which can be used as well as addition and multiplication.

Given the nature of the problem, practice at developing intuition is of more value than a formal developed algorithm, but understanding how much time is taken on solving problems in ordinary arithmetic should develop understanding of more complicated problems in combinatorial optimisation.

New Age factorisation

Mike Richards

mike@z9m9z.demon.co.uk

One of the celebrated "Holy Grails" of Computational Number Theory has, for a long time, been an efficient algorithm to factorise seriously big numbers. Ideally, the time taken by such an algorithm should be some polynomial expression in the number of digits of the number N to be factorised; that is, it should be polynomial in $\log N$. Back in the Dark Ages (before 1960) the best algorithms known took on the order of $N^{\frac{1}{4}}$ (as a comparison, trial division by a list of primes takes $N^{\frac{1}{2}}$). This is of little use when trying to factorise, for example, numbers on the order of 10^{200}.

In the last 30 years, however, a number of promising algorithms have appeared, taking us much closer to the goal of an efficient algorithm. We've not quite reached polynomial in $\log N$ yet, as far as I know at the time of writing, but we're almost there. In this article, I'm going to describe the simplest of these, for want of a better term, New Age algorithms. More sophisticated variants do exist, but they all use the same basic, simple, trick:

Suppose we are trying to factorise N. We want to find integers x and y such that

$$\begin{aligned} x &\not\equiv \pm y \pmod N \\ x^2 &\equiv y^2 \pmod N. \end{aligned}$$

Then, since $x^2 - y^2 = (x+y)(x-y)$, we get a non-trivial factor of N by looking at $\gcd(N, x+y)$.

Of course, we won't find x and y by looking at random integers. The trick, which all of the modern algorithms use, is to look for congruences of the form

$$x_k^2 \equiv (-1)^{e_{0,k}}\, p_1^{e_{1,k}} \dots p_m^{e_{m,k}} \pmod N$$

where the p_i are "small" primes. If we find enough of these relations, we can find an expression

$$\sum_{k=1}^{k=n} \epsilon_k\,(e_{0,k}, e_{1,k}, \dots, e_{m,k}) \equiv (0, \dots, 0) \pmod 2$$

with $\epsilon_k \in \{0,1\}$ and at least one $\epsilon_k \neq 0$. Then let

$$\begin{aligned} (\nu_0, \dots, \nu_m) &= \frac{1}{2}\sum_{k=1}^{k=n} \epsilon_k\,(e_{0,k}, \dots, e_{m,k}) \\ x &= \prod_{k=1}^{n} x_k^{\epsilon_k} \end{aligned}$$

$$y = (-1)^{\nu_0} p_1^{\nu_1} \dots p_m^{\nu_m}$$

and we see that

$$\begin{aligned}
x^2 - y^2 &\equiv \prod_{k=1}^{n} x_k^{2\epsilon_k} - \prod_{l=1}^{m} p_l^{2\nu_l} \pmod N \\
&\equiv \prod_{k=1}^{m} (-1)^{\epsilon_k e_{0,k}} p_1^{\epsilon_k e_{1,k}} \dots p_m^{\epsilon_k e_{m,k}} - \prod_{l=1}^{m} p_l^{2\nu_l} \pmod N \\
&\equiv (-1)^{\sum_{k=1}^{m} \epsilon_k e_{0,k}} \prod_{l=1}^{m} p_l^{\sum_{k=1}^{m} \epsilon_k e_{l,k}} - \prod_{l=1}^{m} p_l^{2\nu_l} \pmod N \\
&\equiv \prod_{l=1}^{m} p_l^{2\nu_l} - \prod_{l=1}^{m} p_l^{2\nu_l} \pmod N \\
&\equiv 0 \pmod N
\end{aligned}$$

This will give us a factorisation unless $x = \pm y \pmod N$, which in practice rarely happens. We call the p_i the *factor base*, and the different algorithms get the congruences and the factor base in different ways.

The particular algormithm I will describe is the "Continued Fraction" method, usually known as **CFRAC**. It is based on work by Legendre, Kraitchik, Lehmer and Powers, and was developed by Brillhart and Morrison. Here, we try and find small values of t such that

$$x^2 \equiv t \pmod N$$

If we find such a pair (t,x), it is reasonable to suppose that t will be a product of primes in our factor base, giving us a congruence.

If t is small and $x^2 \equiv t \pmod N$, then $x^2 = t + kd^2N$ for some coprime, squarefree, k and d, and so

$$\left(\frac{x}{d}\right)^2 - kN = \frac{t}{d^2}$$

will be small. Therefore, x/d will be a good approximation to $\sqrt{kN}$. However, it is well known that continued fraction expansions give, in a certain sense, the "best" rational approximations to a real number. This is the idea behind CFRAC.

We compute the continued fraction expansion for $\sqrt{kN}$ for a number of squarefree natural numbers k such that $kN \equiv 0$ or $1 \pmod 4$. We can do this using simple, efficient, integer arithmetic. This gives us a good rational approximation P/Q say. We then try to factor the *small* integer

$$\begin{aligned}
t &= P^2 - Q^2kN \\
|t| &< 2\sqrt{kN}
\end{aligned}$$

in our chosen factor base. If we succeed, we have a congruence. If we fail, we try again with a different k.

Without going into technical details, primes in the factor base should be small, and kN should be a square (mod p). Implemented properly, this algorithm uses sub-exponential time (that is, it is worse than any polynomial-time algorithm, but better in the long run than any exponential-time algorithm); unfortunately it also requires sub-exponential space (translation: a *lot*). The most modern factorisation algorithms use sub-exponential time and polynomial (in $\log N$, of course) space, which is a big improvement, but they are technically much more sophisticated.

For more details, and a description of these better algorithms, the best book I know of is "Computational Number Theory" by Professor Henri Cohen, from which the algorithm described here was taken.

Taking the square root of a function

Ian Collier

imc@ecs.ox.ac.uk

The square root of what?

David Singmaster once gave a talk at the Invariants and afterwards asked this question: What is the square root of the exponential function? In other words, can you define a function f such that for all x, $f^2(x)$—that is, $f(f(x))$—is equal to e^x? He did not give the answer straight away so I attempted it and devised the solution below.

Choose a function, any function...

Choose $x_0 < 0$. Let $\theta : (-\infty, x_0] \to (x_0, 0]$ be bijective. Let

$$f(x) = \begin{cases} \theta(x) & \text{if } x \leq x_0 \\ e^{f^{-1}(x)} & \text{if } x > x_0 \end{cases}.$$

Then $f : \mathbb{R} \to (x_0, \infty)$ is a total bijective function satisfying:

(i) for all $x \in \mathbb{R}$, $f(f(x)) = e^x$.

(ii) for all $x \in \mathbb{R}$, $x < f(x) < e^x$.

(iii) if θ is continuous and increasing then so is f.

For proofs of the properties of f, let a sequence $\{x_n\}$ be defined with x_0 as before by setting $x_1 = 0$ and, for $n \geq 0$, $x_{n+2} = e^{x_n}$.

The function f can be seen to be total and bijective by considering the intervals $(-\infty, x_0]$ and $(x_n, x_{n+1}]$ for each $n \geq 0$. It is given that f maps $(-\infty, x_0]$ bijectively (and totally) to $(x_0, 0]$, and therefore that f^{-1} exists on $(x_0, 0]$ and maps it bijectively to $(-\infty, x_0]$. The function $x \mapsto e^x$ maps the latter interval bijectively to $(x_1, x_2]$. Hence f^{-1} maps $(x_0, 0]$ bijectively to $(x_1, x_2]$. By induction on n in this manner, it is easily shown that f maps $(x_n, x_{n+1}]$ bijectively to $(x_{n+1}, x_{n+2}]$ for each $n \geq 0$.

The above properties may be proved as follows:

(i) Choose $x \in \mathbb{R}$. Then $f(x) > x_0$ (as it is in the image of f) and so $f(f(x)) = e^{f^{-1}(f(x))} = e^x$ as required.

(ii) The result follows from the facts that f maps $(-\infty, x_0]$ to $(x_0, x_1]$ and $(x_n, x_{n+1}]$ to $(x_{n+1}, x_{n+2}]$, and $x \mapsto e^x$ maps $(-\infty, x_0]$ to $(x_1, x_2]$ and $(x_n, x_{n+1}]$ to $(x_{n+2}, x_{n+3}]$.

(iii) (a) If θ is increasing then so is θ^{-1} and hence f^{-1} on $(x_0, x_1]$. If f^{-1} is increasing on $(x_n, x_{n+1}]$ for $n \geq 0$ then f is increasing on this interval, since $x \mapsto e^x$ is increasing and $f(x) = e^{f^{-1}(x)}$ for each x in $(x_n, x_{n+1}]$. It then follows that f^{-1} is increasing on $(x_{n+1}, x_{n+2}]$, and hence (by induction) that f is increasing everywhere.

(b) If θ is continuous then f is continuous on each interval $(x_n, x_{n+1}]$ for $n \geq 0$ as well as on $(-\infty, x_0]$ (that is, f is continuous everywhere except possibly at x_n for each $n \geq 0$) (this follows by induction in a manner identical in form to that used to prove part (a) above). It is required to show then that for each x_n, $\lim\limits_{\substack{x \to x_n \\ x > x_n}} f(x) = f(x_n)$.

If θ is continuous, increasing and bijective then $\lim\limits_{x \to -\infty} \theta(x) = x_0$ and $\theta(x_0) = 0$. The latter is because if $\theta(x_0) < 0$ then θ cannot be both bijective and increasing (for if it is increasing then for all $x < x_0$, $\theta(x) < 0$ and 0 is not in the image of θ). To prove the former, let ϵ be a positive small number (less than $-x_0$). Because θ is bijective, there exists x_ϵ such that $\theta(x_\epsilon) = x_0 + \epsilon$. Because θ is increasing, for all $x < x_\epsilon$, $x_0 < \theta(x_\epsilon) < x_0 + \epsilon$ so that $|\theta(x) - x_0| < \epsilon$.

In the same manner also it is shown that for all $n \geq 0$, $\lim\limits_{\substack{x \to x_n \\ x > x_n}} f(x) = x_{n+1}$ and $f(x_{n+1}) = x_{n+2}$, given that f is continuous, increasing and bijective on each interval $(x_n, x_{n+1}]$. The combination of these results gives that f is continuous at each x_n, and hence f is continuous everywhere.

What does Taylor say about that?

Well that solution is all very well, but it doesn't give you an answer that you can type into a computer. It doesn't even guarantee you a differentiable result. Fortunately, the next time David Singmaster came to Invariants he offered another solution, devised by a chemistry student at Cambridge (would you believe) called William T. Tutte in 1935 (Tutte did become a professional mathematician 10 years later and eventaully became an eminent professor in Canada).

Firstly, let us attempt to find a fixed point of the function f. Suppose that $f(\alpha) = \alpha$. Then clearly $e^\alpha = f^2(\alpha) = f(\alpha) = \alpha$. We can solve numerically this equation to find a complex number α, as follows (unfortunately, there is no real number satisfying this equation). Let $\alpha = re^{i\theta}$. Then $re^{i\theta} = e^\alpha$, which is $e^{r\cos\theta}e^{ir\sin\theta}$. Taking the moduli and the arguments separately, we have that $r = e^{r\cos\theta}$ and $\theta \equiv r\sin\theta \pmod{2\pi}$. From the second equation we can take the value $r = \frac{\theta + 2n\pi}{\sin\theta}$ and substitute into the first, and solve the resulting equation using Newton's method. We get about $0.318132 \pm 1.337236i$ (and countably many other solutions).

Taylor says that

$$f(\alpha + x) = f(\alpha) + f'(\alpha)x + \frac{f''(\alpha)}{2!}x^2 + \frac{f'''(\alpha)}{3!}x^3 + \cdots$$

(plus a small error term if the series is truncated), provided the series converges. Since we know $f(\alpha)$, we can find the values of $f'(\alpha)$ and so on by repeatedly differentiating the equation $f^2(\alpha) = e^x$ and solving the resulting equations. This should be done by computer, as it is rather messy to do by hand. The first few derivatives of $f(f(x))$ are as follows (the e^x part is much easier!).

$0:\ f(f(x))$

$1:\ f'(f(x))f'(x)$

$$\begin{aligned}
2:\ & f'(f(x))f''(x) + f''(f(x))f'(x)^2 \\
3:\ & f'(f(x))f'''(x) + 3f''(f(x))f''(x)f'(x) + f'''(f(x))f'(x)^3 \\
4:\ & f'(f(x))f^{\prime 4\prime}(x) + 3f''(f(x))f''(x)^2 + 4f''(f(x))f'''(x)f'(x) + f^{\prime 4\prime}(f(x))f'(x)^4 \\
& \quad + 6f'''(f(x))f''(x)f'(x)^2 \\
5:\ & f'(f(x))f^{\prime 5\prime}(x) + 10f''(f(x))f'''(x)f''(x) + f^{\prime 5\prime}(f(x))f'(x)^5 \\
& \quad + 10f^{\prime 4\prime}(f(x))f''(x)f'(x)^3 + 5f''(f(x))f^{\prime 4\prime}(x)f'(x) + 10f'''(f(x))f'''(x)f'(x)^2 \\
& \quad + 15f'''(f(x))f''(x)^2f'(x)
\end{aligned}$$

Unfortunately, the derivatives get longer and contain higher numbers in an approximately exponential fashion, in such a way that after the 26th derivative, which contains 2436 terms, the numbers get too high for the program to handle (the program I used copes with numbers up to 2^{63}, which is about 9×10^{18}).

Anyway, since we know e^{α}, and that $f(\alpha) = \alpha$, we can calculate each derivative of f in turn at α. This gives a Taylor series

$$f(\alpha + x) = \alpha + a_1x + a_2x^2 + a_3x^3 + \cdots$$

where the coefficients are (approximately) as follows.

$$\begin{aligned}
a_1 &= 0.919970 + 0.726782i \\
a_2 &= 0.272218 + 0.0862241i \\
a_3 &= 0.0178072 + 0.00260275i \\
a_4 &= 0.00327273 - 0.000640497i \\
a_5 &= -0.00183400 + 0.00288580i \\
&\vdots
\end{aligned}$$

I have so far calculated the series up to a_{29}, whose modulus is about 6.6×10^{-7}, and it is clear that the coefficients are decreasing. This means that the Taylor series converges at least for values of x such that $|x| < 1$, and that if $|x| < 1$ then the result can be calculated to six digits or so. I have no mathematical proof that the series converges, but one reference—the proceedings of the conference held in honour of Professor W. T. Tutte on the occasion of his sixtieth birthday, at the University of Waterloo, July 5–9, 1977—claims that such a proof exists.

Unfortunately, since α is at a distance greater than 1 from the real line it is a little difficult to test the function on real numbers—and in any case the function probably maps real numbers to complex numbers rather than real ones (of course, when you apply f again you get a real number back). However, we can do a couple of tests on complex numbers, such as the following.

$$\begin{aligned}
f^2(i) &= f(0.249917 + 0.852231i) = 0.540302 + 0.841471i \\
f^2(\tfrac{1+i}{2}) &= f(0.928871 + 0.573106i) = 1.446889 + 0.790439i
\end{aligned}$$

These both gave the correct answers to within six digits.

This power-series technique can be used for almost any function g as long as $g'(\alpha)$ is neither zero nor -1. If $g'(\alpha)$ is real and positive then the resulting f will map the real line into itself. Obviously you don't meet a problem like this every day, but you never know. . .

A Helpful Guide to Courses

Mike Richards and Erica Neely[1]

mike@z9m9z.demon.co.uk, some0140@sable.ox.ac.uk

In the confusion of your first three or four years at Oxford, you might find discovering what to take is a bit tricky. You could, I suppose, read the Exam Decrees or the synopses for the courses, but who truly has time to do that? So we have compiled this guide to courses, which we hope you will find, if not useful, at least entertaining (NB: these courses truly do exist).

Complex Analysis: This is just like Real Analysis, but simpler.

Graph Theory: The study of tennis.

Set Theory: The study of unchanging things.

Mechanics: How to fix cars.

Quantum Mechanics: How to fix quanta.

Applied Probability: How to fix cards.

Surreal Arithmetic: Fish.

Physics: The study of Coca-Cola and other things that go fizz in the night.

Theoretical Physics: The study of Coca-Cola *without drinking any*!

Mathematical Biology: The study of mathematicians and how they work. (Or don't.)

Mathematical Ecology: The study of Mathematical Institutes.

Group Theory: Working together to understand one another's problems.

Topology: The study of coffee cups and doughnuts (this is a graduate course).

Turbulence: The art of stirring coffee (also known as "Applied Topology").

Statistics: The art of lying.

Field Theory: Watching grass grow…

Cryptography: see Necrology.

Rings and Fields: Engagement celebrations.

Groups and Fields: Orgies (a popular course).

Representation Theory: The study of American politics. (Mike did this one—I know better.)

Viscous Fluid: College soup?

Wave Theory: The art of saying farewell.

Mathematical Models: Juliette, Catherine, Erica and Jo. (Mike did this one. He's 3/4 right.)

[1] Parenthetical remarks by Erica Neely.

Proof Theory: The study of alcohol.

Computer Science: A contradiction in terms.

Linear Regression: The theory of devolution.

Integration: The art of equality. (Being from the southern US, I have problems with this.)

Differentiation: The art of inequality. (I'm good at this, though.)

Mathematical Methods: Rarely real, frequently complex, never rational, and often imaginary.

Chaos Theory: All of the above. At once.

The life and works of John von Neumann

Chris Dickson

kebl0110@sable.ox.ac.uk

Janos Neumann was born in Budapest, Hungary, 4 days before the start of 1904. His father, a successful banker, later had two other sons. He lived with parents, grandparents, aunts, uncles and cousins, learning French and German from infancy. Before too long, his photographic memory (hypermnesia) was spotted, so his father had a library installed in the house which Janos lapped up. He adored history and artistic works which left questions unanswered. As a not-very-committed Jew, he attended a Lutheran school and studied mathematics at an accelerated rate; in 1919 a Communist government took power and the margitta Neumann family as they had become after buying a minor aristocratic title left for Austria, spending time in Vienna and on the coast. He spent his undergraduate careers—three of them, often two at once—at the Universities of Budapest, Berlin and Zurich, studying mathematics, chemistry and chemical engineering; he took his Ph. D. in mathematics at the age of 22. He was then named Privat Dozent, a very senior research position for one so young, and held that title in Berlin and Hamburg for 4 years. He referred to himself as Johann Neumann von Margitta at that time, sometimes Johann von Neumann.

In 1929 he was offered a post lecturing Quantum Theory at Princeton for a semester and accepted, only taking time out to marry his girlfriend, Mariette Koevesi. He lectured there for three years, but was often difficult for his weaker students to follow. Then the Princeton Institute for Advanced Study opened in 1933 and he was named the youngest professor of a distinguished group—later to include Leray, Dirac and Einstein. His wife had a daughter, Marina, in 1935, but two years later she divorced him to remarry physicist J. B. Kuper, though they stayed on good terms and John von Neumann (to which he had Anglicised his name) brought Marina up from between the ages of 12 and 18. He remarried within a couple of years of his divorce with a childhood sweetheart, Klara Dan, who had just recently been divorced herself; John wrote her saccharine-sweet love letters and got moody, often terse ones in reply. Their marriage seems to have been one of mixed happiness, due to John often spending more time on his work, with all the travel that was involved, than being 'a normal family' with his wife; perhaps their dog, 'Inverse', and the child that they brought up brought them together.

John was a hearty type, keen on rich food and an occasional hard drinker who was keen on practical jokes, limericks and verbal gags, some very baudy, others sarcastic; politically mildly conservative, his driving of automobiles was aggressive and possibly reckless, with accident and incident on occasion. He made a number of small but very kind acts, sending money to people whom he knew who deserved it. He had a particular penchant for children's toys, particularly construction ones. His relationship with his wife was frequently very strained when his work got the better of him. That said, his style at work was quiet and thoughtful, though he often would not stick at a problem that wasn't interesting him.

From 1925 to 1940 von Neumann made significant contributions to many areas, tending towards mathematics with easily-seen real-life applications. His work on Game Theory started with a 1928 article, 'Zur Theorie der Gesellschaftspiele' or the Theory of Parlour Games. After that, his work on 'rings of operators'—von Neumann algebras—was published in 1932 and he made advances in lattice theory in 1935–37. Other areas he worked on were logic, set theory and group theory. During the war, von Neumann did consulting work for the Navy Bureau of Ordnance and he spent the first half of 1943 in and around London. In 1944 he wrote 'Theory of Games and Economic Behaviour', probably the quintessential work on Game Theory, with Oskar Morgenstern, an Austrian economist then at Princeton; it took the field of economics by storm, although readership was very limited. It is an ambitious and very formula-laden book—their treatment of games for more than two players makes it drag. More recent work has showed that their work on two-player games, particularly zero-sum ones for which the minimax strategy was identified for the first time, has been most useful.

John von Neumann also did a good deal of work for International Business Machines, the computer firm now best known for its Personal Computers. He proposed a machine that used the same memory for data and instructions, the controlling processor interpreting the binary digits it finds as instructions or data depending upon what it expects. This arrangement of computer, with a central processor linked directly to the main storage (memory) by a very high-speed link (input, output and address buses) in the mainframe, and slower hardware links to bulk storage (disk) and a communication controller which deals with input and output, is referred to as a von Neumann machine. This design was used as far back as EDVAC (the Electronic Discrete Variable Automatic Computer) and has been used ever since.

In late 1945, General Henry Arnold of the Army Air Force met with directors of Douglas Aircraft to discuss the establishment of what became known as Project RAND, an organisation 'to further and promote scientific, educational and charitable purposes, all for the public welfare and security of the United States of America'. In fact, the RAND Corporation that was established first studied Inter-Continental Ballistic Missiles, then studied fantastic, bizarre, outlandish and sideline ideas dreamt up by the Air Force. Over the next eight years or so, very few people who made advances in game theory weren't working at RAND Corporation. One of the more popular RAND publications was John D. Williams' 1954 guide for the interested layman, 'The Complete Strategist'. This didn't completely serve to change public opinion of the RAND Corporation; it was still thought of as 'thinking about the unthinkable'—considering the best ways to wage war, possibly with weapons of mass destruction, what the effects of war would be and how best to survive, cope and prosper after war. Over the years, some of the projects that my namesake Paul Dickson criticised RAND for following included semantics, surfing, Soviet Union bricks and social groupings of monkeys. Economists and other social scientists were hired as well, many of whom worked on developing game theory.

Von Neumann's involvement with the RAND Corporation began in 1948 when he was hired as an informal consultant; it is recorded that during lunchtimes of his occasional visits there he played the then-popular game Kriegspiel, which was a simplification of a complicated war game popular in Prussia, played using three chess boards. He was not able to find a 'solution' to the Prisoner's Dilemma (devised by Merrill Flood and Melvin

Dreshler, and first attempted in practice by UCLA's Armen Alchian and RAND's John Williams) for no 'solution' exists. Parallels are easily drawn from it to the nuclear A-bomb and H-bomb situation, where co-operation implies not building bombs and defection implies building them, and John would be classified as a strong advocate of defection. John was a strong advocate of what was known as 'preventive war', under the opinion that if both Americans and Russians possessed such powerful nuclear weapons, the side to use them first (or even pose a strong enough threat to use them) would gain such a massive advantage in the war that ensued that it might be beneficial to launch an unprovoked attack. Thus they would have an immense metaphorical stick to threaten the Russians with if they ever acted out of accordance with US wishes. This thought might possibly have been encouraged by his presence at Bikini atoll where on two occasions in July 1946, atomic bombs were exploded. These were only the fourth and fifth occasions ever, and the first to be announced beforehand; he was invited to them along with other scientific and non-scientific dignitaries. The heat from the explosion could be felt very strongly by people fully ten miles away.

John von Neumann became busier over the years with his University work and even after RAND raised his 1951 daily working wage to $100, he gave up working for them in 1955. The work that was otherwise involving him included designing a computer for studies on the H-bomb in 1951 and other forms of consultancy that had to stop in late 1954 when he was personally appointed as a commissioner to the Atomic Energy Commission; a role he was proud to take on, flattered that he was 'entrusted with a high governmental position of great potential influence in directing large areas of technology and science, an activity of great national importance'. He was still against the disassembly of nuclear weapons, fearing that if America disarmed in response to Russian promises to do so, the Russians might well disarm only to rearm in secret, and having two secret nuclear arsenals in the world did not favour his country. He was announced as the Atomic Energy Commision's delegate to the President's Special Committee on Disarmament inaugurated by President Eisenhower on the 5th of August, 1955.

After that, things seemed to go downhill for von Neumann as his physical health started to deteriorate. He fell on a slippery floor, hurting his left shoulder. This pain was not to go away; after further tests a secondary cancer of the prostrate gland was identified. Theories that this was brought on by the nuclear tests he had attended seem to have little credibility. Further aches and pains followed, lesions were found on his spine and early in 1956 he was confined to a wheelchair for the rest of his life. That February, Eisenhower presented him with the Medal of Freedom and later the first ever Fermi Award (a gold medal and a then huge $50,000) for contributions to the field of atomic energy. His mother died in July and John was in a very bad way after that, his hypermnesia coming back to provide him with many haunting memories of the past; his nights were traumatic and his rambling proclamations confused. His immense depression got worse and worse; he very unexpectedly seriously took on Catholic views after consultation with a Benedictine monk, Father Anselm Strittmatter, but remained terrified of death. He died on the 8th of February in 1957.

Both his wife, Klara, and his daughter by his first marriage, Marina, survived him. Neither had any direct interest in his work, though both met with success in related subjects; Klara worked with a population research study at Princeton. Though employed for her knowledge of languages, she excelled in the statistical side of the work. Later, she worked as a programmer for computers installed at the Aberdeen Proving Ground and Los Alamos. She was one of the first computer programmers ever and had her husband to thank for his considered suggestions to IBM which included using digital machines operating using binary digits and working using software in the form of stored programs as opposed to hard-wired circuits for each different problem. Marina, who married at the age of around 21, graduated first in liberal arts from Radcliffe College and became an economist, later a vice-president of General Motors, despite claiming to have no predilection for mathematics.

So Janos Neumann, despite living little over the age of fifty, made many advances in branches of mathematics that are still widely in use and heavily acknowledged today. Furthermore he developed game theory and the stored-program computer, two concepts that have shaped all our lives immeasurably. No wonder Jacob Bronowski described him as '. . . a genius, in the sense that a genius is a man who has two great ideas.'

The I-Spy Book of Mathematicians

Mike Richards and Erica Neely

mike@z9m9z.demon.co.uk, some0140@sable.ox.ac.uk

The mathematician is a lesser spotted—though often striped—species found in a variety of habitats. Specimens are seldom early risers, and their coloration tends to be in varying shades of drab, though there are, of course, exceptions. There are many subspecies of mathematician, some of which we list here for your convenience and amusement.

Senior Mathematician (*Professor Emeritus*)

Noted for its enthusiasm and droning call, this species is usually only found with its head in the clouds. Colouring and cleanliness vary, often depending on the presence of a mate.

College Tutor (*Tutorus Collegius*)

This is a common species whose markings vary greatly in colour and style. One often finds members of the class Sub-bachelorius Articus attempting to impress the Tutorus Collegius with their imaginative but hastily constructed displays. Hybrids are generally discouraged but occasionally occur.

Visiting Tutor (*Tutorus Visitsus*)

A fairly common species, the Tutorus Visitsus tends to migrate long distances and seldom creates permanent nests. It is easily recognised by its distinctive droning voice and the lost and slightly bewildered look it has.

Tutor on Sabbatical (*Tutorus Sabbaticallius*)

Seldom seen in its natural habitat, the Tutorus Sabbaticallius usually mimics the Tutorus Visitsus in migration habits. It is a fairly undistinctive breed and can be hard to distinguish from the Tutorus Collegius.

Member of Invariants (*Saddus Saddus*)

Saddus Saddus is a dying species, noted for its ability to consume large quantities of biscuits and coffee, and its seeming compulsion to collect bits of card. It is a social creature with frequent gatherings, and can be recognised by its distinctive call: "Mao-Mao". (Note: Scholars speculate as to whether the new trend of alcohol consumption is partially responsible for the falling numbers, but as of yet there is no real proof one way or another.)

Invariant Committee Member (*Saddus Suckerus*)

A large and ever-growing species, Saddus Suckerus is currently headed by the solitary member of the species Saddus Suckerem, a small but vocal creature known as "The

President". Saddus Suckerus members are frequently seen flitting around in states of extreme agitation or exchanging gossip; they are often found around bowls of water. Saddus Suckerus is gradually replacing Saddus Saddus as the dominant species.

Undergraduate Student (*Sub-bacheloricus Articus*)

This is one of the most numerous of species, despite seeming to be quite short-lived. Its members are usually found in large flocks which may perch for several hours before dispersing. Often criticised for being a noisy species, colouring and habitats vary considerably.

Graduate Student (*Post-bacheloricus Articus*)

While rarer than the Sub-bacheloricus Articus, this species is still more common than many. Though it rarely associates with Saddus Saddus or Saddus Suckerus, it tends to result in a long and fulfilling relationship when it does. It sometimes mimics the Tutorus Collegius, with varying degrees of success; the life-span of the Post-bacheloricus Articus varies considerably.

The Institute Receptionist (*Receptiona Institutia*)

The solitary member of a hard working species, the Receptiona Institutia is rarely spotted except in flight. Although it adopts a deceptively relaxed attitude—often leading to the misconception that it is lazy—in fact the Receptiona Institutia is a vital component of the ecosystem.

Finals! Finals!

Jonathan Young

The Mathematics Faculty at the University of Crazytown has adopted an unusual method of presenting marks for candidates' attempts at Finals papers. Each paper contains eight questions which may be attempted and solutions are given an integer mark out of 25. The mark for the paper is given in terms of sum, sum of squares and alpha, beta and gamma counts.

Definitions: Let x_i be the mark for question i ($i = 1, \ldots, 8$). Then

$$\begin{aligned} Sum &= \sum_{i=1}^{8} x_i \\ Sumsq &= \left\lfloor \left(\sum_{i=1}^{8} \frac{x_i^2}{10} \right) + \frac{1}{2} \right\rfloor \\ \alpha &= \sum_{i=1}^{8} \chi_{[21,25]}(x_i) \\ \beta &= \sum_{i=1}^{8} \chi_{[13,20]}(x_i) \\ \gamma &= \sum_{i=1}^{8} \chi_{[10,12]}(x_i) \end{aligned}$$

where $\chi_{[a,b]}(x) = \begin{cases} 1 & \text{if } x \in [a,b] \\ 0 & \text{otherwise} \end{cases}$
and $\lfloor x \rfloor$ is the greatest integer which is less than or equal to x.

Little Johnny attempted paper B1. He looked through the questions in order, attempting only those whose question numbers were prime. Each solution that he wrote was judged to be better than the previous one. His marks were recorded as follows.

Sum	$Sumsq$	α	β	γ
70	129	2	1	1

What were his exact marks for each question? Can you show your answer is unique?

Closing Time—The Solution

You may remember the five logic students, Aristotle, Boole, Cayley, Descartes and Euler, and their tutor, Professor Truth, who became inebriated and forgot which colleges they all attended. In case you don't, since the last issue of *The Invariant* was some time ago, a summary of the problem is this. The professor made three guesses at which colleges the students attended: firstly, Aristotle at Oriel, Boole at New, Cayley at Lincoln, Descartes at Magdalen and Euler at Keble; secondly, Aristotle at New, Boole at Lincoln, Cayley at Magdalen, Descartes at Oriel and Euler at Keble, and thirdly, Aristotle at Lincoln, Boole at Keble, Cayley at Magdalen, Descartes at New and Euler at Oriel. On each occasion the professor was incorrect, but he was told that his guesses became progressively better. The final piece of information was that Cayley attends neither Magdalen nor Keble.

Since each guess is incorrect, three correct colleges is the most that the professor could have achieved on the third guess; hence one correct college is the most that he could have achieved on the second guess: since Magdalen was wrong there can only be four correct colleges in the second and third guesses together. Therefore none of the colleges was correct in the first guess.

Suppose the third guess contained three correct colleges. Since Euler does not go to Keble (because of the first guess), he must go to Oriel. Then Descartes could not go to Oriel and must therefore be at New. This leaves Aristotle at Lincoln and Boole at Keble being the only possibilities, and only Magdalen is free for Cayley, which is incorrect. This contradiction shows that only two colleges were correct in the third guess.

Suppose the correct college in the second guess were Aristotle's—namely, New. Then, since Cayley does not go to Magdalen or Keble, and cannot go to Lincoln because the first guess was entirely wrong, the only choice left is Oriel. After that it is impossible to choose two correct colleges from the third guess.

Suppose the correct college in the second guess were Boole's—namely, Lincoln. Then Cayley must go to either New or Oriel, again leaving it impossible to choose two correct colleges from the third guess.

Since Cayley does not go to Magdalen, and Euler does not go to Keble, the only remaining possibility for the correct college in the second guess is that Descartes goes to Oriel. This means that from the third guess we must choose Aristotle going to Lincoln and Boole going to Keble. Cayley does not go to Magdalen and therefore must go to New, which leaves Euler at Magdalen.

—The Editor

Crossword

Almost all of the clues and answers in this crossword have some remote connection to mathematics, but as there is at least one member who is a chemist I added a couple of chemistry questions. Some of the clues are straightforward; many are cryptic (warning: a couple of the answers make only the vaguest of sense in English). The author of the first correct solution to reach the Editor may be eligible for a small prize.

■	1	■	2	■	3	■	4	■	■	■	5	■	6	■
7									■	■	8			
■		■		■		■		■	9	■		■		■
10					■	11								
■	■	■		■	12	■		■		■		■		■
■	■	13									■	14		
■	15	■		■		■		■		■	16	■		■
17							■	18						
■		■		■		■	19	■		■		■		■
20			■	21									■	■
■		■	22	■		■		■		■		■	■	■
23									■	24			25	
■		■		■		■		■	26	■		■		■
27				■	■	28								
■		■		■	■	■		■		■		■		■

1 A distinguished ring member (4)
2 An unchanging member of society (9)
3 $17\frac{1}{2}\%$ of a large tank of liquid (3)
4/19 $\int f(x,y)d(x,y) = \int \left(\int f(x,y)dy \right) dx$ (7,7)
5 Of matter, one of three (not including Bose-Einstein condensates) (5)
6 One stage in demonstrating the truth of alcohol content upon a stair (5,4)
7/18 $\exists c \in (a,b) \bullet f'(c) = \dfrac{f(b)-f(a)}{b-a}$ (4,5,7)
8 Part of an expression or of the academic year (4)

9 A line between two segments of a circle—not the one on the right (4,5)
10 Arctic co-ordinates? (5)
11 A function one-to-one and 27 (9)
12 Defines the elements of a group at the power station (9)
13 1.5 times the society's birthday (9)
14 ψ (3)
15 Coinciding exactly when superimposed (9)
16 A square (5-4)
17 A value with limits leapt (7)
18 See 7
19 See 4
20 After which an oval is named (3)
21 Science of numbers to be done by people in rotation (can this describe your lecture list?) (5,4)
22 An inert gas (5)
23 Consisting only of the fifth element (4,5)
24 Some brain putting data into a computer program (5)
25 One invertible ring member (4)
26 Chip placed unseen initially within a computer (3)
27 See 11
28 Your tutor may use it for marking (3,6)