## MATHS REVIEW



## The Maths Behind

Cryptography!
Prime numbers and their use in cryptography

## The Stowe Maths Review

The Stowe Maths Review is a magazine that gives an insight into maths at Stowe!

## Contents 9$)=(3+2,-7 \cdot 9)=(5,2$

Prove by contradiction that the square roots of prime numbers are irrational by Oliver Vince Page 3

- Cryptography and Prime Numbers by Anna -Wilson Page /4

Complex Numbers aren't that complex by Toby Lawrance Page 6
 Mathematics and Language by Alfred Cliff Page 8 The Basel Problem by Hugo Barnet Page 10 Number Theory by lIly Riskin Page 13 - 1 Infinity by Sean Page 16 Pi as Power Series By Mryadsan page 20 Versicle Stretch Lessons page 24 Gaussian Group! Page 26 What Does an Atom Look Like Page 28

$$
11-2+2
$$

## Local Maximum Sessions Page 29

$3 x z)=4 y\left(3 y y+x^{2}\right.$ Maths Jokes and Riddles Page 30

$$
\binom{27+5 x y}{2 \pi} \vec{k}
$$

$$
\text { in Maths Crossword Page } 31
$$

Special thanks to:
d(Allmembers of the Gaussian Group.
Mr Moiler who is always open to new ideas and whose passion for mathematics is a source of inspiration for us all? All the maths teachers in the department.
Adam/Gabriel and Jåmeŝ̂earfe for their support.
Mr Giles Cuddy for arranging the first Mathematics/and/History joint event (Geometry of Hate) for the lower school.
d. Kanav Bhatnàgaífor designing this magazine and putting everything $2 x^{2}-5 x$ together for us.

Tori Roddy for helping us to publish this magazine.

## Prove by contradiction that the square roots of prime numbers are irrational

By Oliver Vince
A prime is a number that is divisible only by itself and I (e.g. 2, 3, 5, 7. II). An irrational number is a number that cannot be made by dividing 2 numbers: therefore. it is expressed as decimal with an infinite number of digits to the night of the decimal point. without repetition leg. Pi/ $\pi=3.141592653$. $\qquad$

## Proof by Contradiction

If we say that ' $p$ ' is a prime number and let's assume that $V_{p}$ is national.
$V_{p}$ is therefore rational and it can be represented as the ratio of 2 integers.
Therefore it can also be represented as the ratio of 2 co-prime integers 12 integers that have no factors in common). so an irreducible fraction.
$\nabla_{p}=a / b \leftarrow$ cannot be reduced

- So if we square both sides $\mu=a^{2} / b^{2}$.
- Then multiply both sided by $b^{2} b^{2} p=a^{2}$.

This tells us that ' $n$ ' must be a factor of ' $a^{22}$.

- " $a$ " written as a product of primes ( $f=$ factors): $a=\| x \nmid 2 \ldots x$ in.
- ' $a^{22}$ written as a product of primes: $\left.\left.a^{2}=(f) x q^{2} \ldots f n\right)(f) x \not q^{2} \ldots f_{n}\right)$.

Therefore ' $\beta$ " is also a factor of ' $a$ " $\rightarrow$ " $a$ " us a multiple of ' $\beta$ ' $\rightarrow a=K p(K=$ some integent.
Substituting this back into $b^{2} \rho=a^{2}$
$b^{2} \rho=\left(k_{p}\right)^{2}$
$b^{2} p=k^{2} p^{2}$
$b^{2}=K^{2} p$ (dividing by $\left.{ }^{\prime} p^{\prime}\right)^{\prime} \rightarrow b^{2 \prime}$ is a multiple of ${ }^{\prime \prime} p^{\prime} \rightarrow b^{\prime \prime}$ is a multiple of ${ }^{\prime} \beta^{\prime}$.
This proves that $V_{p} \neq a / b$ (so $V_{p}$ is irrational) since " $b^{\prime}$ "s a multiple of ' $\beta$ " and ' $a$ " is a multiple of ' $a$ '. the numerator and the denominator can be divided by

# Cryptography and Prime Numbers 

## 3227731347

Prime numbers have fascinated mathematicians for centuries, showing up in surprising places in nature, such as the shape of shells, and being the reason four leaf clovers are so rare. Yet despite all the work invested in them, and all the progress made, prime numbers continue to challenge mathematicians and many problems remain unproved centuries on, such as The Goldbach conjecture' that positive integers greater than 2 can be. expressed as a sum of two primes, or The twin prime conjectures that there are an infinite number of twin primes.
Prime number become ever more important as computers develop due to their use in cryptography. Prime numbers are important for public key cryptography, because a very large number is used as a public key to encrypt a file, but in order to decrypt the file the prime factors of the large number must be worked out This is both very difficult and time consuming as there seems, currently, to be no easy method for prime factorisation This means the large number used to encrypt a file can be publicly known without compromising the safety of a file. Although technically given enough time the prime factors could be worked out, Some estimates suggest it would take a modern super computer longer than the current age of the universe to work out a 256-bit factorisation. It can be proved that- any positive integer greater than 1 is equal to a product of prime numbers.
In this proof, the number of primes in a product must be allowed to be one, since a prime number is itself the product of one prime. If $n$ is a positive integer then for $n \geq 2$, let $P(n)$ be the statement that $n$ is equal to a product of prime numbers. 49

Suppose that $P(2), \ldots, P(n)$ are all true, meaning every integer between 2 and $\%$ $n$ has a prime factorisation. If $n+1$ is prime, then it must have a prime factorisation. If $n+1$ is not prime, then by the definition of a prime number there is an integer a dividing $n+1$ such that $a \neq 1$ or $n+1$. Writing $b=(n+1) / a$ then
$n+1=a b$ and $a, b \in(2,3, \ldots, n)$

By assumption, $P(a)$ and $P(b)$ are both true i.e., $a$ and $b$ have prime factorisations. Say
$a=p_{1} \ldots p_{k}, b=q_{1} \ldots q_{l}$,
where all $p_{i}$ and $q_{i}$ are prime numbers. Then
$n+1=a b=p_{1} \ldots p_{k} q_{1} \ldots q_{l}$.
This is an expression for $n+1$ as a product of prime numbers.
$P(2), \ldots, P(n) \rightarrow P(n+1)$. Therefore, $P(n)$ is true for all $n \geq 2$, by Strong Induction.
It is also important for public key cryptography that prime factorisation is unique- there is only one way of writing an integer as a product of primes. This is because it essentially means there is only one way to decrypt a file-making the decryption more difficult.
5 535 It is logical, that the larger a number is the harder it is to find its prime factors, so usually prime numbers with more than 200 digits are required for secure transmission of sensitive information. The discovery of new, larger, primes are considered so important there is a prize of $\$ 150,000$, to the first individual or team who find a prime number with at least $100,000,000$ decimal digits. There are many ways to find large prime number such as searching for the prime number terms in Fibonacci's sequence, as well as methods to test numbers to see if they are primes, such as a variant of Fermat's Little Theorem, Miller's test.

2010
5 As quantum computers develop, cryptography will have to develop to stay ahead and the deputy director of the Institute for Quantum
Computing at the Uniyersity of Waterloo, estimates a one in two chance that quantum computing will break a public key crypto by 2031.
However that will not be the end of the use of prime number in cryptography, merely the start of a new era.


# Complex Numbers aren't that Complex 

By Toby Lawrance

Complex numbers provide solutions to equations that don't normally have a solution. Such as $x^{2}+1=0$ where $x= \pm \sqrt{-1}$ but... we have a problem here! Thew -1 doesn't exist, you can't square root a negat number. Except...you can and the answer is rephesented by he letter $i$. Where $i^{2}=-1$ and therefore $i=\sqrt{-}$ This is known as an imaginary number the lack of real world equivalent. A complenuber is made of a real part and an imaginary part, for instance: The roots of the equation: $(x-3)^{2}+4=0 \operatorname{aros}-3 \pm 2 i$ and tada! We can now solve a ton more equations, and all we had to do was add a letter and new system. Complex numbers can be used for a bunch of things, but they're notable for a few, most people have seen the equation: $e^{i \pi}+1=0$ and potentially knowit as Euler's formula. The proof for which provides interestin insights into complex logarithms. But firstly.. Complex numbers can be represented on an form $x+i y$ such that the complex number 3 the location $(3,2)$ on our grid. As shown belo

|  |  |
| :---: | :---: |
|  |  |
|  | ${ }^{(3,2)}$ |
|  | $\cdots$ |
| - | - |
| - | - ${ }^{5}$ |
|  |  |
|  |  |
|  |  |

This provides us with some additional info... namely, the angle it makes with the positive $x$-axis and it's magnitude which is its length, in this instance, the magnitude is $\sqrt{3^{2}+2^{2}}=\sqrt{13}$ and the angle from the positive $x$-axis, known as its "argument" which is measured in radians, is: atan $\left(\frac{2}{3}\right)=$ 0.588

From this we can write our complex in another form: $r e^{i \theta}$ where $r$ is our magnitu and $\theta$ is our argument.
Therefore, we can rewrite $3+2 i$ as $\sqrt{13}$ which may look slightly worse but can lead on to Euler's equation. Where we ask, "Ho would we represent -1 as a complex number of the form $r e^{i \theta}$ ?" and thus we convert ( $-1,0$ ) to Complex form.

In a regular sense, the value is $-1+0 i$ and therefore, our magnitude is 1 and our argument is Pi, so what would this look like? $e^{i \pi}$ exactly as 1 times anything is itself. Therefore... we can say that $e^{i \pi}=-1$ which exactly the same as $e^{i \pi}+1=0$ And thus we've illustrated Euler's formula, giving a brief introduction to Complex numbers in the process.

## Mathematics and Languap The Philosophy of Mathematics as a Universo Language

It has been a field of thought explored by many an interested individual who has been left alone long enough to consider it, "why is it that we cannot all" learn a single language?". The language barrier is one that many strive to. overcome through learning another language. However, it often doesn't occurito us that there is quite a different subject that has enabled the free communication of knowledge without the struggle of learning a secondlanguage. Mathematics is that which has been used to solve problems of physics and logic since its origination in the Middle East.

Should one be of a mind to visit France, then, assuming they know no French, they would be quite at the mercy ofthé chance that a passing Frenchman speaks English. Of coursé, while many French speakers do speak English, there is nothing more reassuring than the possibility of a universal language. This language is mathematios Wherever one travels, they will always know the truths of maths: two in addition loanother two makessfour. The idea that there is a shared knowledge and truth no matter where one goes, and whoever one converses with, is certainly a comro itiug she.

Nevertheless, we find ourselves now at a barrier in this trail of thought. Too soon we häve encountered a barciedr: though mathematics will forever hold true, wherever one goes, it is not directly utilised as a language. In fact one must be capable of speaking another language in order to express the mathematics which I have already claimed to be a language in itself. So where am I coming from? How, do I believe, canwe bring the language of maths into the scene of the other dominant world languages? Wêll, mathematics is more than just a general purpose language. A general purpose language is one such as Spanish, French or English. The communication through mathematics is not for general purpose, rather it is what is known as a discipline specific language.

The disciplines within maths are used to communicate data on a pus scale, which can be read by anyone, regardless of their general-purpose) ang ?ge. Mathematics when used to communicate as a discipline specific langta? leads to extraordinary feats of human accomplishment. The most ob youls being the field of Information and Communication Technology (ICT) whigh
envelops computers, machines and coding. Mathematics has allowed or all digital and virtual advancement, which in those advancements themselves mankind has found new means of communication.

The conclusion of this essay is that mathematics has, and continues to, offer people everywhere a common ground of communication, even if that language is a discipline-specific one. What mathematics can give us is a universal understanding of logic and the principles of communication.

# The Basel Problem 

By Hugo Barnet

$$
1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}+\frac{1}{25}+\frac{1}{36}+\ldots
$$

It seems like a simple problem, which many would go about by adding up the first few terms and trying to develop a pattern... However, some A-level students might have the bright idea of summing up some geometric series. Sounds straightforward, doesn't it? However, one quickly realizes it is not so easy. In fact, it took one of the greatest mathematical minds in human history to solve it - Leonhard Euler. It was called 'The Basel Problem' after Euler's hometown. The mathematician Pietro Mengoli first proposed this in 1644, and it took about 90 years to solve. Fairly long time, huh?

Personally, I really enjoyed the proof of this problem because it combines a couple of different areas of mathematics and also once you get your head around it, the proof seems dead easy. In this article, I will attempt to make you, the reader, understand the beauty behind the proof. Hopefully it will inspire you to look past some of the tiresome and boring mathematics that is taught in schools and start to see it as the vibrant, creative subject it really is.

So to start the proof, we need to look into a bit of trigonometry.
Particularly, the Sinx curve. As many of you will already know, the curve $f(x)=\sin x$ will look like this


When they ask you in the exam: What is the solution to $f(x)=\sin (x)$, you would be right in saying $\pi$, but then again you would be right in say $2 \pi$ or $3 \pi$. You would be right in saying "any integer number $\pi$ ", because the $\sin (x)$ curve passes the x-axis infinitely many times at the coordinates $(\mathrm{k} \pi, 0)$ where k is an integer. For those saying to themselves, "what on earth is this guy is talking about"- as one advances through the world mathematics we start to use the unit system of radians instead of degrees. It very simple, 360 degrees is $2 \pi, 180$ degrees is $\pi$ ect.

$$
\sin (x)=x(x \pm \pi)(x \pm 2 \pi)(x \pm 3 \pi)(x \pm 4 \pi) .
$$

We can use this to find a polynomial for $\sin (\mathrm{x})$. If the solution for $\sin (\mathrm{x})$ is K $\pi$ then we can make this polynomial. Through some basic algebra we can manipulate the equation so that we can get $\sin (\mathrm{x})$ in the form of

$$
\begin{aligned}
& \sin (x)=x\left(x^{2}-\pi^{2}\right)\left(x^{2}-4 \pi^{2}\right)\left(x^{2}-9 \pi^{2}\right)\left(x^{2}-16 \pi^{2}\right) \ldots \\
& \sin (x)=x\left(\frac{x^{2}}{\pi^{2}}-1\right)\left(\frac{x^{2}}{4 \pi^{2}}-1\right)\left(\frac{x^{2}}{9 \pi^{2}}-1\right)\left(\frac{x^{2}}{16 \pi^{2}}-1\right) \ldots
\end{aligned}
$$

If we mutiply out this polynonial we can get the a seires with all the cofficent to the $\mathrm{x}^{\wedge} 2$

$$
\sin (x)=x\left(1-x^{2}\left(\frac{1}{\pi^{2}}+\frac{1}{4 \pi^{2}}+\frac{1}{9 \pi^{2}}+\frac{1}{16 \pi^{2}} \cdots\right)+\ldots\right)
$$

The next step to this problem requires some higher knowledge on the $\sin (\mathrm{x})$ curve that most of the reader will be unfamilar with. To get more familiar, one should look up taylor seires. Basically, the sin function can be written as an infinite sum.

$$
\sin (x)=x-\frac{x^{3}}{3!}+\frac{x^{5}}{5!}-\frac{x^{7}}{7!} \cdots
$$

Euler started by imagining another seires very similar to the $\sin (\mathrm{x})$ but this time he called it the $P(x)$. It was essentially the sin curve but with one less in the powers of $X$. Euler was then able to say that $\mathrm{xP}(\mathrm{x})$ was equal to the polynomial $\sin \mathrm{x}$.

$$
\begin{gathered}
P(x)=1-\frac{x^{2}}{3!}+\frac{x^{4}}{5!}-\frac{x^{6}}{7!} \cdots \\
x P(x)=x-\frac{x^{3}}{3!}+\frac{x^{5}}{5!}-\frac{x^{7}}{7!} \cdots \\
x P(x)=\sin (x) .
\end{gathered}
$$

If that is true then $\mathrm{xP}(\mathrm{x})$ must be equal to the polynomail we previously wrote down. Therefore

$$
\begin{aligned}
& x p(x)=x\left(1-x^{2}\left(\frac{1}{\pi^{2}}+\frac{1}{4 \pi^{2}}+\frac{1}{9 \pi^{2}}+\frac{1}{16 \pi^{2}} \cdots\right)+\cdots\right) \\
& \left.p(x)=1-x^{2}\left(\frac{1}{\pi^{2}}+\frac{1}{4 \pi^{2}}+\frac{1}{9 \pi^{2}}+\frac{1}{16 \pi^{2}} \cdots\right)+\cdots\right) \\
& 1-\frac{x^{2}}{3!}+\frac{x^{4}}{5!}+\frac{x^{6}}{7!} \cdots=1-x^{2}\left(\frac{1}{\pi^{2}}+\frac{1}{4 \pi^{2}}+\frac{1}{9 \pi^{2}}+\frac{1}{16 \pi^{2}} \cdots\right)+ \\
& \frac{x^{2}}{3!}=x^{2}\left(\frac{1}{\pi^{2}}+\frac{1}{4 \pi^{2}}+\frac{1}{9 \pi^{2}}+\frac{1}{16 \pi^{2}} \cdots\right) \\
& \frac{\pi^{2}}{3!}=1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16} \cdots \\
& \frac{\pi^{2}}{6}=\sum_{r=1}^{\infty} \frac{1}{R}
\end{aligned}
$$

## Number Theory

## Introduction

The Number Set is a set of positive integer numbers $1,2,3,4,5,6,7, \ldots$, Devoted primarily to the studies of integers and is sometimes called "The Queen of Mathematics" due to its foundational place in the discipline. It consists of the study of the properties of the whole numbers. Prime and Prime factorization are especially important in number theory, as are many functions such as the divisor function, Riemann zeta function, and totient function. Excellent introductions to number theory may be found in Ore (1988) and Beiler (1966).

Main difficulty in proving relatively simple results in number theory prompted no less an authority than Gauss to remark that "it is just this which gives the higher arithmetic that magical charm which has made it the favourite science of the greatest mathematicians, not to mention its inexhaustible wealth, wherein it so greatly surpasses other parts of mathematics." Gauss, often known as the "prince of mathematics," called mathematics the "queen of the sciences" and considered number theory the "queen of mathematics" (Beiler 1966, Goldman 1997). In contrast to others branches of mathematics, many of the problems and theorems of number theory can be understood by laypersons, although solutions to the problems and proofs of the theorems often require a sophisticated mathematical background.

Until the mid-20th century, number theory was considered the purest branch of mathematics, with no direct applications to the real world. The advent of digital computers and digital communications revealed that number theory could provide unexpected answers to real-world problems. At the same time, improvements in computer technology enabled number theorists to make remarkable advances in factoring large numbers, determining primes, testing conjectures, and solving numerical problems once considered out of reach.

In today's world, the Modern number theory is a large subject that is divided into subjects that include elementary number theory, algebraic number theory, analytical number theory, geometric number theory, and probabilistic number theory. These categories reflect the methods used to address problems concerning the integers.

## From Pre-History Through Classical Greece

Near the beginning of civilisation, people had understood the idea of 'multiplicity' and so had taken the first steps toward a study of numbers. It is known that the understanding of numbers existed in ancient Mesopotamia, Egypt, China, and India, for tablets, papyri, and temple carvings from these early cultures have survived. A Babylonian tablet known as Plimpton 322 (c. 1700 bc ) is the main point. In modern notation, it displays number triples $\mathrm{x}, \mathrm{y}$, and z with the property that $\mathrm{x} 2+\mathrm{y} 2=\mathrm{z2}$. One such triple is $2,291,2,700$, and 3,541 , where $2,2912+2,7002=3,5412$. This reveals a degree of number theoretic agreement in ancient Babylon.

## Diaphantus

An author of a book - Arithmetica. The equations are called Diophantine Equations of which the solutions must bewhole numbers. For example, Diophantus asked for two numbers, one a square and the cube, so that the sum of their squares is square itself. In today's symbols, he sought integers $x, y$, and $z$ such that $(x 2) 2+(y 3) 2=z 2$. Finding real numbers is easy satisfying this relationship (e.g., $x=\sqrt{ } 2$, $y=1$, and $z=\sqrt{ } 5$ ), however, the requirement that solutions be integers makes the problem more difficult. (One answer is $x=6, y=3$, and $z=45$.) Diophantus's work strongly influenced the future mathematics.

## Number Theory in the East

Chinese and Indian scholars proposed their contribution to the theory. They were so motivated by questions of astronomy and the calendar, the Chinese mathematician Sun Zi tackled multiple Diophantine equations. He asked for a whole number that when divided by 3 leaves a remainder of 2 when divided by 5 leaves a remainder of 3 , and when divided by 7 leaves a remainder of 2 (his answer: 23). Almost a thousand years later, Qin Jiushao (1202-61) gave a general procedure, now known as the Chinese remainder theorem, for solving problems of this sort.

## Modern Number Theory

From 1400 to 1650, as mathematics flowed from the Islamic world to Renaissance Europe, the amount of attention number theory got decreased. Important advances in geometry, algebra, and probability have occurred not to mention the discovery of both logarithms and analytic geometry. But number theory was a minor subject and therefore only of a recreational interest.

## Pierre de Fermat

Pierre de Fermat (1601-65), has changed the perception a French magistrate who had time and a passion for numbers. Although he published little, Fermat posed the questions and identified the issues that have amended number theory ever since. For example:

1. In 1640 he proposed what is known as Fermat's little theorem, that if $p$ is prime and $a$ is any whole number, then $p$ divides evenly into $a p-a$. so, if $p=7$ and $a=12$, the far-from-obvious conclusion is that 7 is a divisor of $127-12=35,831,796$. This theorem is one of the great tools of modern number theory today
2. In 1638 Fermat stated that every whole number could be expressed as the sum of four or fewer squares. He claimed to have a proof but did not share it.

Uncharacteristically, Fermat gave a proof of this final and last result. He used a technique called 'infinite descent' that was ideal for demonstrating the impossibility. The logical strategy assumes that there are whole numbers satisfying the condition in question and then generates smaller whole numbers satisfying it as well. Reapplying the argument over and over, Fermat produced an endless sequence of decreasing whole numbers. But this is impossible, as every set of positive integers must contain the smallest member. By this contradiction, Fermat concluded that no such numbers could exist in the first place. Despite Fermat's unique, number theory still was relatively rejected perhaps because of his reluctance to supply the proofs.

## Prime Number Theorem

One of the largest achievements of 19th-century mathematics was the prime number theorem. First, you designate the number of primes less than or equal to by $\pi(n)$. Thus $\pi(10)=4$ because $2,3,5$, and 7 are the four primes not exceeding 10. Similarly $\pi(25)=9$ and $\pi(100)=25$. Next, consider the proportion of numbers less than or equal to $n$ that are prime-i.e., $\pi(n) / n$. Clearly, $\pi(10) / 10=0.40$, meaning that 40 percent of the numbers not exceeding 10 are prime.

The prime number theorem identifies at least one, thereby provides a rule for the distribution of primes among the whole numbers. The theorem says that, for large $n$, the proportion $\pi(n) / n$ is roughly $1 / \log n$, where $\log n$ is the natural logarithm of $n$.

## Prime number theorem

(illustrated by selected values $n$ from $10^{2}$ to $10^{4}$ )

| $n$ | $\pi(n)=\begin{aligned} & \text { number of primes less } \\ & \text { than or equal to } n \end{aligned}$ |  | proportion of primes <br> $=$ among the first $n$ numbers | $\frac{1}{\log n}=$ | predicted proportion <br> of primes among the first $n$ numbers |
| :---: | :---: | :---: | :---: | :---: | :---: |
| $10^{2}$ | 25 |  | 0.2500 |  | 0.2172 |
| $10^{4}$ | 1,229 |  | 0.1229 |  | 0.1086 |
| $10^{6}$ | 78,498 |  | 0.0785 |  | 0.0724 |
| $10^{8}$ | 5,761,455 |  | 0.0570 |  | 0.0543 |
| $10^{10}$ | 455,052,511 |  | 0.0455 |  | 0.0434 |
| $10^{12}$ | 37,607,912,018 |  | 0.0377 |  | 0.0362 |
| $10^{14}$ | 3,204,941,750,802 |  | 0.0320 |  | 0.0310 |

## Number Theory in the 20th Century

The 20th Century saw an explosion in number theoretic research. As well the classical and analytic number theory, scholars now explored specialised subfields such as algebraic number theory, geometric number theory, and combinatorial number theory. The concepts became more abstract and the techniques more sophisticated. Therefore, the subject had grown beyond Fermat's dreams.

A legendary figure in 20th-century number theory was Paul Erdős (1913-96), a Hungarian genius known for his deep insights, his vast circle of collaborators, and his personal oddities. At age 18, Erdős published a much more simplified proof of a theorem of Chebyshev saying that, if $n \geq 2$, then there must be a prime between $n$ and $2 n$. This was the first in a string of number theoretic results that would span most of the century. In the process, Erdős-who also worked in combinatorics, graph theory, and dimension theory-published over 1,500 papers with more than 500 collaborators from around the world. He achieved this success while constantly travelling from one university to another in pursuit of new mathematics. It was not uncommon for him to arrive, unannounced, with the declaration that "My brain is open" and then to plunge into the latest problem with gusto. Twentieth-century number theory reached a high climax in 1995, when Fermat's last theorem was proved by the Englishman Andrew Wiles, with timely assistance from his British colleague Richard Taylor. Wiles succeeded where so many had failed with a 130-page proof of incredible complexity, one that certainly would not fit into any margin.

## $\infty$ INFINITY $\infty$

## BySean Carslaw Tricot.

Infinity is big: Infinitely big. But what do we know about this fundamental concept of mathemátics and what are it's uses.

Getting there

- Luckily, it is probably the simplest

Going through the big numbers wé always think we;are getting closer to infinity but we are always as far as we always were...

## $18,446,744,073,709,551,615$

This interesting number comes. from and ancient tale about chess where 3000 years ago in ${ }^{-}$India, King Belkib is asked to put a grain of rice on the first square of a chessboard and double the number of grains on the next square of the chessboard. The king accepted. But what he didn't know was that he had to put $2^{n}$ on the $n^{\text {th }}$ square. This meant that on the last square, he had to put $2^{63}$ grains of rice. The number that we are talking about is the total number of grains of rice that should be on the chessboard. This may seem like a fairly big but not too impressive number when talking about grains of rice but the amazing fact is that since one grain of rice weight approximatively 0.04 g , the king needs to put 738 billion tons of rice on that chessboard. Enough to feed humanity for centuries. थ. Googol, 10100 :

Googol or sometimes google is much, much bigger than the last number (approx. 1019).
number on this page since its value is only (only!) 10 to the power of 100 . But, this number is, also.VERY big. It is deemed to be much bigger than the number of particles in the umiverse (protons + neutrons + eléctrons); estimated to be approximatively 1080

## Googolplex, 10 googol:

OK. Now that we know what google is, what if we made an even bigger number? Hmm... Right, let's have 10 to the power of... google! To put this into perspective, this is in effect a 1 followed by a google zeros!

## $3 \uparrow \uparrow \uparrow 3$

Now here we have a strange and MUCH, like, seriouslỳ much bigger number than googolplex. This number is written with the Knuth up arrow notation. To explain: take $5 \uparrow 3$. In this case, this is read: '. take three fives and multiply them* together' $=5^{3}=125$.

Now take $5 \uparrow \uparrow 3$ : this is 5 to the power of 5 to the power of 5 , which amounts to $5^{3125}$, this is basically a 'tower' of powers of 5 with 3 - 'levels' already much, much bigger than google.
So what is $3 \uparrow \uparrow \uparrow 3$ ? Well, $3 \uparrow \uparrow \uparrow 3$ can also be written $3 \uparrow \uparrow 3 \uparrow \uparrow 3$. This is a
tower of powers of 3
Now we can conclude from our. explanations that $3 \uparrow \uparrow 3$ is 3 with 3 lévels of powers', $3^{27}$. So therefofe $3 \uparrow \uparrow \uparrow 3$ is a tower with 327 levels of powers of 3 . That is 7625 billion levels! A massive change from googolplex!. .:


## Graham's number :

This number is the biggest number ever used to solve a theoretical problem. Compared to the previous number, it doesn't have 4, 1000 nor everi a billion arrows but an unimaginable number of these! This number was used to solve a thieoretical problem to... colour a hypercube. A geometrical shape with the same properties as a cube but in more than 3 dimensions.

To construct this rtumber, take the. previous number ( $3 \uparrow \uparrow \uparrow 3$ ), this is the number of arrows between the threes of the next number, which is the number of artows between the threes of the next number...etc. Now repeat these steps until the $65^{\text {th }}$ iteration, Graham's number.

## ... Infinity? ${ }^{*}$

Going though these numbers getting bigger and bigger we get the impression that we should'be getting closer to infinity but'we aree
still-at our starting point, because infinity is ... infinitely big!

Paradoxes

## Dichotomy paradox:

Imagine you are" thro
something hardrat someone y yoủ really don't like, let's say you are throwing a rock. Now, befofé that rock reaches that certain person it need́s to trayellá certain distance.
$\because$ Before it travels that distance, it travels half. And before travelling that, it'travels half of that, and so on infinitely. But will it'then never reach this certain person? No need: to pick up another rock, here fs the proof:
let S be the infinite sum:
$\mathrm{S}=1+1 / 2+1 / 4+\cdots$
$\therefore$ Now, factorise by $1 / 2$ :
$\mathrm{S}=1 \mathrm{w}+1 / 2(1+1 / 2+1 / 4+\ldots)$
Notice how the sum in the
parenthesis is the same as the first so we can write:
$S=1 ;+1 / 2 S$
$2 \mathrm{~S}=2+\mathrm{S}$
solve:
$2 s-s=2$
$\mathrm{S}=2$
This proves how this infinite sum ${ }_{\bar{\sigma}}$ 2. Not verýtinfifinite if you ask me!

- The box gets fuller but is always empty :

In Greek mythology, the Danaids were condemned to fill a pierced bucket with water which let oủt more water than they put in. Impossible. But what if you were tasked to fill a box with ping pong balls and for every ten you put in only one came out? Would you accept the challenge? Be careful because when infinity is in the - mix, it's easy to go wrong... So,

- during the first minute, you throw
$10^{\circ}$ balls in; the first ball comes out* .. your sides are infinitely small BUT* $\rightarrow$ there are 9 ballis in the box. You decide to speed up and in half. $\because$ : These cancel.
a minute; you throw ten more balls; ball number 2 comes.outi $\rightarrow$ there are 18 balls in the box. So each time you add 9 balls. Each time you throw 9 balls in in half the time of the previous throw. Still following?. Now doing this to $\because:$ infinity, you add 9 balls in $11^{1}+1 / 2+$ $1 / 4+\ldots$ ) minutes. As concluded. from the last paradox, that allamounts to 2. This isn't as simple . as it may seem... On throw 1, ball 1 comes out, on throw 2 , ball 2 comes out. C So in 2 minutes, you' add an infinite amouint of balls; BUṪ, an infinite amount of balls come out. So in the end, the box you are filling is always... empty!


## Step by:step :

Draw an isosceles right angled triangle on the floor, now stand at an angle but make sure that it is not the right angle. You want to go to the other non-right:angle in the triangle. You would opt to go along the hypotenuse, the shortest distance. But is it really? Let's ste. Take the two non-hypotenuse sides and divide them into two and create a step with the two parts adjacent to the right angle. Repeat . this with each of these new lines until you cannot distinguish the steps, do it infinitely. With this your triangle only appears to have one hypotenuse and that is it. If each of the original sides were 1 meter, than $2=\sqrt{ } 2$. Now you are thinking: What? This is impossible, impossible to reduce this distance - of 2 to its square root by simply stepping it infinitely. The catch here is that by stepping infinitely,

PROVE $\quad \frac{\pi}{2}=\sum_{0}^{\infty} \frac{k!}{(2 k+1)!!}$
$(2 k+1)!!$ means $(2 k+1)(2 k-1)(2 k-3) \ldots$
We know
$(2 k+1)!=(2 k+1)(2 k)(2 k-1)(2 k-2)(2 k-3) \ldots$
$=(2 k+1)(2 k-1)(2 k-3) \ldots(2 k)(2 k-2)(2 k-4) \ldots$
$=(2 k+1)(2 k-1)(2 k-3) \ldots 2^{k}(k)(k-1)(k-2) \ldots$
$=(2 k+1)!!2^{k} k!$
So
$(2 k+1)!=(2 k+1)!!2^{k} k!$
$\Rightarrow(2 k+1)!!=\frac{(2 k+1)!}{2^{k} k!}$
So
$\frac{\pi}{2}=\sum_{0}^{\infty} \frac{k!}{(2 k+1)!!}=\sum_{0}^{\infty} \frac{k!}{\frac{(2 k+1)!}{2^{k} k!}}=\sum_{0}^{\infty} \frac{2^{k} k!k!}{(2 k+1)!}$
Lets call $\frac{\pi}{2}=\sum_{0}^{\infty} \frac{2^{k} k!k!}{(2 k+1)!} \quad E 1$
Using the definition of n choose r
$\binom{n}{r}=\frac{n!}{(n-r)!r!}$
$\Rightarrow\binom{2 k}{k}=\frac{(2 k)!}{(2 k-k)!k!}=\frac{(2 k)!}{k!k!}$ lets call this B
$\frac{\pi}{2}=\sum_{0}^{\infty} \frac{2^{k} k!k!}{(2 k+1)!}=\sum_{0}^{\infty} \frac{2^{k} k!k!}{(2 k+1)(2 k)!}=\sum_{0}^{\infty} \frac{2^{k}}{(2 k+1)} \cdot \frac{k!k!}{(2 k)!}$
Substituting B into E 1, we get
$\sum_{0}^{\infty} \frac{2^{k}}{(2 k+1)}\binom{2 k}{k}^{-1}$

## Generating Functions

$A$ Generating Function $f(x)$ is a power series
$f(x)=\sum_{0}^{\infty} a_{n} x^{n}$
whose coefficients give the squence $\left\{a_{0}, a_{1}, a_{2} \ldots\right\}$

An example,
Consider the infinite series $f(x)=\sum_{n=0}^{\infty} x^{n}=1+x+x^{2}+x^{3} \ldots$.
The generating function for this series is
$f(x)=\frac{1}{1-x}$, This is trivial, using G.P and realizing Binomial
Expansion of $\frac{1}{1-x}=(1-x)^{-1}$
Now,
What is the generating function for $\sum_{0}^{\infty} \frac{2^{k}}{(2 k+1)}\binom{2 k}{k}^{-1}$ ?

Theorem
Generating function $\mathrm{A}(t)=\varsigma\left(\frac{4^{n}}{2 n+1}\binom{2 n}{n}^{-1}\right)$
$=\frac{1}{t} \sqrt{\frac{t}{1-t}} \arctan \sqrt{\frac{t}{1-t}}$

Proof
Let $\mathrm{A}_{n}=\left(\frac{4^{n}}{2 n+1}\binom{2 n}{n}^{-1}\right) \Rightarrow \mathrm{A}_{n+1}=\left(\frac{4^{n+1}}{2 n+3}\binom{2 n+2}{n+1}^{-1}\right)$
$=\frac{4 \cdot 4^{n}}{2 n+3} \cdot\left(\frac{(2 n+2)!}{(2 n+2-(n+1)!(n+1)!}\right)^{-1}=\frac{4 \cdot 4^{n}}{2 n+3} \cdot\left(\frac{(2 n+2)!}{(n+1)!(n+1)!}\right)^{-1}$
$=\frac{4 \cdot 4^{n}}{2 n+3} \cdot \frac{(n+1)!(n+1)!}{(2 n+2)!}=\frac{4 \cdot 4^{n}}{2 n+3} \cdot \frac{(n+1) n!(n+1)!}{(2 n+2)(2 n+1)(2 n)!}$
$=\frac{4 \cdot 4^{n}}{2 n+3} \cdot \frac{(n+1) n!(n+1)!}{2(n+1)(2 n+1)(2 n)!}=\frac{2 \cdot 4^{n}}{2 n+3} \cdot \frac{n!(n+1)!}{(2 n+1)(2 n)!}$
$=\frac{2 \cdot 4^{n}}{2 n+3} \cdot \frac{n!(n+1) n!}{(2 n+1)(2 n)!}=\frac{2(n+1)}{2 n+3} \cdot \frac{4^{n}}{(2 n+1)} \frac{n!n!}{(2 n)!}$
$=\frac{2(n+1)}{2 n+3} \cdot \frac{4^{n}}{(2 n+1)} \cdot \frac{n!n!}{(2 n)!}=\frac{2(n+1)}{2 n+3} \cdot \frac{4^{n}}{(2 n+1)} \cdot\binom{2 n}{n}^{-1}$
$A_{n+1}=\frac{2(n+1)}{2 n+3} A_{n}$

$$
\begin{aligned}
& (2 n+3) A_{n+1}=2(n+1) A_{n} \\
& (2 n+2) A_{n+1}+A_{n+1}=2(n+1) A_{n} \\
& 2(n+1) A_{n+1}+A_{n+1}=2(n+1) A_{n}
\end{aligned}
$$

Generating function for $2(n+1) A_{n+1}$ is
$2 \sum_{n=0}^{\infty}(n+1) A_{n+1} t^{n}=2\left(A_{1}+2 A_{2} t+3 A_{3} t^{2}+\ldots ..\right)=2 \frac{d A}{d t}$
Generating function for $A_{n+1}$ is
$\sum_{n=0}^{\infty} A_{n+1} t^{n}=A_{1}+A_{2} t+A_{3} t^{2}+\ldots=\frac{A-A_{0}}{t}$, notice $A_{0}$ is 1
and finally generating function for $2(n+1) A_{n}$ is $2(A+d A / d t)$
this leads to a differential equation,
$2 \frac{d A}{d t}+\frac{A-1}{t}=2 A+2 t \frac{d A}{d t}$, which leads to
$\frac{d A}{d t}+\left(\frac{1-2 t}{2 t-2 t^{2}}\right) A=\frac{1}{2 t-2 t^{2}}$ call this equation (D)
This, first order linear differential equation, can be solved using integrating factor and partial fractions.
(Solving D is left as an exercise to keen students)
Solving (D) we get
$A=\frac{1}{t} \sqrt{\frac{t}{1-t}} \arctan \sqrt{\frac{t}{1-t}}$

Going back to
$\frac{\pi}{2}=\sum_{0}^{\infty} \frac{k!}{(2 k+1)!!}=\sum_{0}^{\infty} \frac{2^{k}}{(2 k+1)}\binom{2 k}{k}^{-1}$
We have show that the generating function for the sequence is
$\frac{4^{n}}{2 n+1}\binom{2 n}{n}^{-1} \quad$ is $\quad \frac{1}{t} \sqrt{\frac{t}{1-t}} \arctan \sqrt{\frac{t}{1-t}}=\sum_{0}^{\infty}\left(\frac{4^{n}}{2 n+1}\binom{2 n}{n}^{-1}\right) \mathrm{t}^{n}$
If we let $t=2^{-1}$
$\sum_{0}^{\infty}\left(\frac{4^{n}}{2 n+1}\binom{2 n}{n}^{-1}\right) \mathrm{t}^{n}=\sum_{0}^{\infty}\left(\frac{4^{n}}{2 n+1}\binom{2 n}{n}^{-1}\right)\left(2^{-1}\right)^{n}=\sum_{0}^{\infty}\left(\frac{4^{n} \cdot\left(2^{-1}\right)^{n}}{2 n+1}\binom{2 n}{n}^{-1}\right)$
$\sum_{0}^{\infty}\left(\frac{(2)^{2 n} \cdot\left(2^{-1}\right)^{n}}{2 n+1}\binom{2 n}{n}^{-1}\right)=\sum_{0}^{\infty}\left(\frac{(2)^{2 n} \cdot(2)^{-n}}{2 n+1}\binom{2 n}{n}^{-1}\right)=\sum_{0}^{\infty}\left(\frac{(2)^{n}}{2 n+1}\binom{2 n}{n}^{-1}\right)$
This is the squence we began with.
So for $t=2^{-1}$
$\frac{1}{t} \sqrt{\frac{t}{1-t}} \arctan \sqrt{\frac{t}{1-t}}=\frac{1}{\frac{1}{2}} \sqrt{\frac{\frac{1}{2}}{1-\frac{1}{2}}} \arctan \sqrt{\frac{\frac{1}{2}}{1-\frac{1}{2}}}=2 \arctan (1)=2 \cdot \frac{\pi}{4}=\frac{\pi}{2}$

## Q.E.D

## Vertical 'Stretch' Lessons

During the course of the year, Mr Yadsan invited keen mathematicians, from all year groups, to his captivating vertical stretch lessons. In these lessons, we learnt complex mathematical topics which tested our ability to apply our existing mathematical knowledge to advanced theories and principles.

## Vertical Stretch Upper School:

We started of our lecture series with Multivariable Calculus. We studied the fundamental concepts of mathematical physics, such as double and triple integrals in Cartesian, Polar and Spherical coordinates. The next lecture series was on numbers and sequences, where we covered, Convergence and Divergence of series and sequences. We proved and used L'Hopital's Rule, Pseries, Integral Test and the Comparison test. In the Lent term, we started on Linear Algebra where we covered, solving system of linear equations using augmented matrices and elementary rowoperations. We progressed to the determinant function and used Cramer's Rule to solve linear systems. We also looked at vector spaces, spanning and linear independence, bases and how to evaluate the points of stability using the determinant of Hessian Matrix.

## Vertical Stretch Lower

 School:Lower school mathematicians covered various topics in mathematics. We looked at some basic Linear algebra, how to add, subtract and multiply matrices and how to work-out the determinant of two by two matrices. Lower school mathematicians also enjoyed and were intellectually challenged by the complex numbers. In this lecture series, we have learnt what a complex number was and why was it needed. Towards the end of this lecture series, Lower school mathematicians were able to tackle advanced level question, such as finding the nth root of complex numbers, such as $z^{5}=(2-3 i)$,For the summer term, Lower school mathematicians will attend a lecture series on Number Theory.


## Gaussian Group

## 2016-2017



This year Stowe's Maths Society, the Gaussian Group, had several meetings covering a broad range of topics from quantum mechanics to the maths behind bottle flipping!

Our meetings started off with a captivating but complex proof which showed that two parallel lines, in fact, meet at infinity. Mind-boggling! In the following week we had a lower school Gaussian group meeting where the connection between mathematics and hate was investigated. In this talk 'Geometry of Hate' we explored: the subtle relationship between mathematics and hate, Hitler and mathematics and how failure in mathematical thinking could lead to fascist movements and civil wars?

In the next a few meetings we focused on the lecture series called "The loss of Truth". We started off with the famous Russell's paradox:

Suppose there is a town with just one barber. In this town, every man either

1) Shaves himself, or
2) Is shaved by the barber.

If the barber shaves himself, then which category does he fall into? Men who shave themselves or Men who are shaved by the barber?

We realized that the Russell's paradox was not simply a philosophical word game but it was a dagger that penetrated the heart of mathematics because it pointed out an inconsistency in the set theory, which is the foundation of mathematics, everything else in mathematics built on it.

In the following lectures we witnessed how hard mathematicians worked, for many years to overcome this difficulty and save Cantor's infinite sets. This paradox was finally solved by redefining the set theory through ZF-Axioms.

Following the loss of truth series, Stoics enjoyed two fascinating talk from Hugo Barnett and Toby Lawrance. Hugo's talk was on number theory where he demonstrated how messages are coded. Toby's talk discussed different bases, as used by the Babylonians, and explained the advantages of us changing from our current base 10 number system to a base 12 number system.

Just before Christmas, the Gaussian group held a quiz night organized by our diligent president Anna Wilson. It was both enjoyable and challenging as all Gaussian group meetings are and it was the perfect way to end a very busy term.

The first meeting in the Lent term was a joint event with the school's second best society: The Quantum Society. The talk was thought provoking and asked profound questions; It was called,
"Machine vs Soul. On the interpretations of Quantum Mechanics".
In the talk we tackled both mathematical and philosophical problems:
Isn't the nature of reality and our perception of it is fascinating? The Observer effect is highly respected and an experimentally verified fact in Quantum Mechanics. When we look at something we change it! Just by looking at it. Do you believe that? Do you believe that you are changing this article simply by reading it! That's what Quantum Mechanics says. Why does Quantum Mechanics abstract observer from reality? Why does it treat human perception as an outsider who perturbs the system? What if we are a part of the truth and not an outsider?

The next event was made up of two talk by members of the Gaussian group. Anna Wilson gave an interesting and inspiring talk on Golden Ratio and its applications in the nature. We have noticed that there is a mathematical reason why the four-leaf clover is hard to find and is lucky. Because four is not a Fibonacci number, therefore it is hard to find in the nature.

Stuart Milner gave a talk on something very simple but we all were amazed to see how mathematical physics played a crucial role in 'bottle flipping'. His talk made the relation between the stability and the centre of mass more visible to all listeners. Adrian Koch then gave a talk on Artificial Intelligence where he linked computer sciences and mathematics.

The last event of this academic year was a distinguished speaker: Dr Marcus Appleby:

## What does an atom look like?’

Dr Marcus Appleby, from Sydney University visited Stowe to give a talk on the Philosophy of Quantum Mechanics, entitled "What does an atom look like?" He is one of the world's leading Quantum Physicist in his field of SIC-POVM (A symmetric, informationally complete, positive operator valued measure). His talk pointed out a fundamental contradiction between our perception and how nature works. He pointed out that:
"On one hand, we are the masters of the universe at subatomic level. We understand it so well that we can even build nuclear bombs. But on the other hand, Quantum Mechanics clearly demonstrates that we don't even know what an electron is. Is it a particle or a wave or both or none? In fact, we don't even know whether is it something physical or it is simply a mathematical modelling?"

This was an extremely profound statement and left the room speechless! This talk was the best way to wrap up the Gaussian groups meeting in this academic year and we'd like to thank Dr Marcus Appleby for giving such a gripping talk.

## 'Local Maximum Sessions'

Oxbridge lessons, where Oxbridge hopefuls gather to tackle MAT and STEP questions.


## Maths Jokes

Why can't a bicycle can' $\dagger$ stand alone?
because it is two-tired.
Statistics show that those who celebrate more birthdays live longer.
A statistician can have his head in an oven and his feet in ice, and he will say that on average he feels fine.

According to my calculations, the problem does not exist.
There are three kinds of mathematicians: those who can count, and those who cannot.

Mathematics consists of 50\% formulas, 50\% proofs and 50\% imagination.

## Maths riddles

Which month have 28 days
All of them

What insect is good with numbers?

An account-ant


Who invented the fractions?
Henry the Eighth

How can you tell that the fractions $x / c, y / c$ and $z / c$ live in a foreign country?

Because they are all over c's.


## Across

2. The point $(0,0)$ on a coordinate plane, where the $x$-axis and the $y$-axis intersect.
3. The vertical axis in a Cartesian coordinate system.
4. Set of two numbers in which the order has an agreed-upon meaning, such as the Cartesian coordinates ( $x$, $y$ ), where the first coordinate represents the horizontal position, and the second coordinate represents the vertical position.
5. One of two or more expressions that are multiplied together to get a product.
6. The line segment connecting two nonadjacent vertices in a polygon.
7. The smallest nonzero number that is a multiple of two or more numbers.
8. A selection in which order is not important.
9. A closed plane figure made up of several line segments that are joined together.
10. A five-sided polygon.
11. A number or symbol, as 3 in $(x+y) 3$, placed to the right of and above another number, symbol, or expression, denoting the power to which that number, symbol, or expression is to be raised.
12. The number of square units that covers a shape or figure.
13. Given or $x^{\wedge} n$, the " $x$ " is the base. The base number gets multiplied by itself the number of times indicated by the exponent, " n ".
14. A constant that multiplies a variable.
15. The sum of the lengths of the sides of a polygon.
16. A mathematical statement that says that two expressions have the same value; any number sentence with an equal sign.
17. The horizontal axis in a Cartesian coordinate plane.

## Down

1. The square root of $x$ is the number that, when multiplied by itself, gives the number, x .
2. The largest number that divides two or more numbers evenly.
3. A letter used to represent a number.
4. A parallelogram with four equal sides.
5. A quadrilateral with four equal sides and four 90 degree angles.
6. Parenthesis, Exponent, Multiplication, Division, Addition, Subtraction.
7. One method for calculating the total number of outcomes in a sample space.
8. A measurement of space, or capacity.
9. The union of two rays with a common endpoint, called the vertex.
10. A quadrilateral with four 90 -degree angles.
11. The side opposite the right angle in a right triangle.
12. A three-sided polygon.

## Thave no special talents.

 I am only passio ately curious:Albert Einstein


