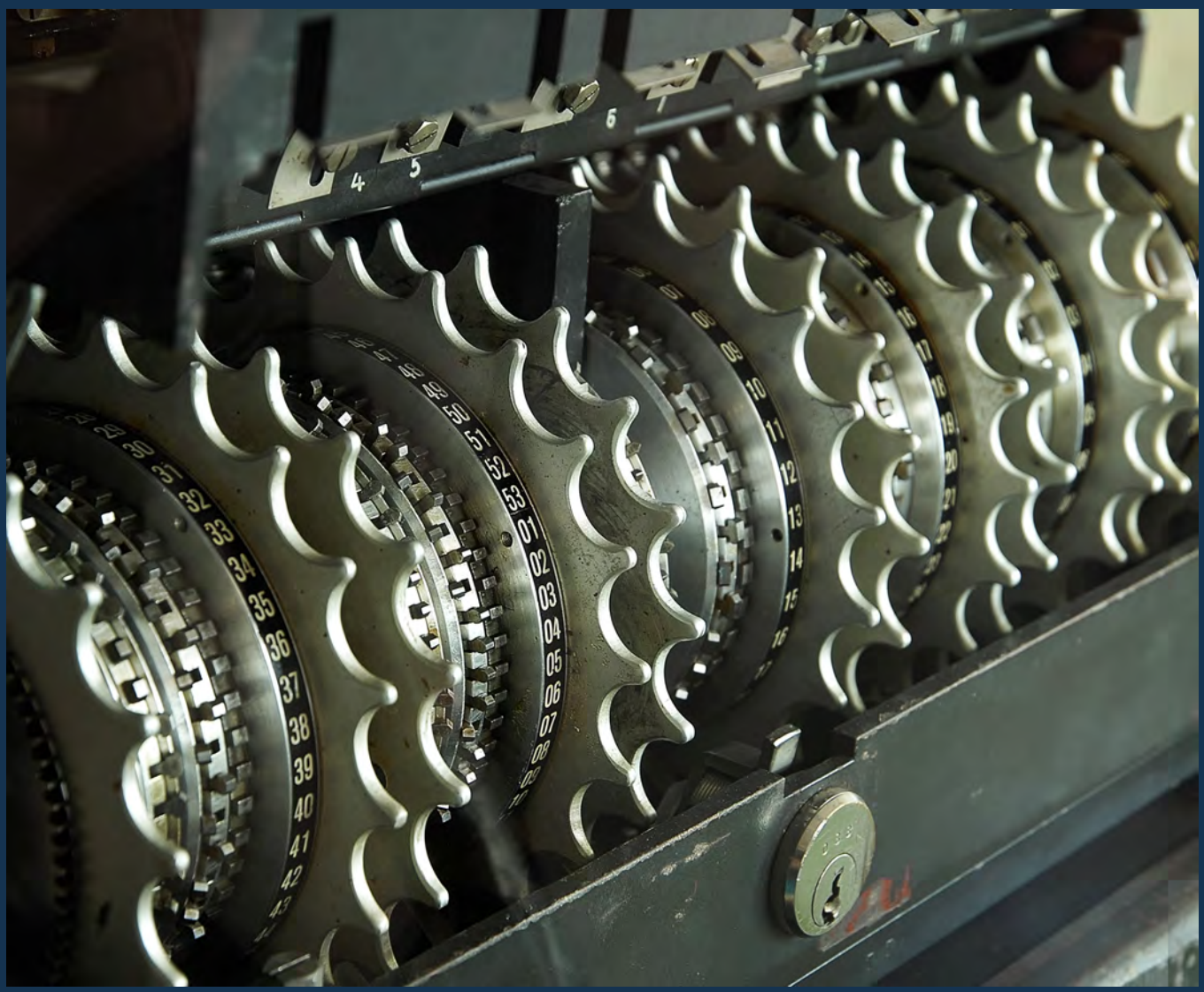
LONDON MATHEMATICAL SOCIETY
EST. 1865

NEWSLETTER

Issue: 472 - September 2017



W.T. TUTTE: CODEBREAKER AND MATHEMATICIAN

CACHING, ENCRYPTION, AND YOUTUBE

PARADING A PANOPLY OF PRIME PROOFS

SUBMISSIONS

The Newsletter welcomes submissions of feature content, including mathematical articles, career related articles, and micro-theses from members and non-members. Submission guidelines and LaTeX templates can be found on newsletter.lms.ac.uk/submissions.

Feature content should be submitted to the editor-in-chief at iain.moffatt@rhul.ac.uk.

News items should be sent to newsletter@lms.ac.uk.

Notices of events should be prepared using the templates on newsletter.lms.ac.uk/submissions and sent to calendar@lms.ac.uk.

For advertising rates and guidelines see newsletter.lms.ac.uk/rate-card.

NEWSLETTER WEBSITE

The Newsletter is freely available electronically through the LMS's website newsletter.lms.ac.uk/.

COVER IMAGE

Courtesy of The National Museum of Computing tnmoc.org.

EDITORIAL OFFICE

London Mathematical Society
De Morgan House
57–58 Russell Square
London WC1B 4HS
T: 020 7637 3686
F: 020 7323 3655
E: newsletter@lms.ac.uk

Charity registration number: 252660

Typeset by the LMS at De Morgan House; printed by Holbrooks Printers Ltd.

CONTENTS

Welcome to the New-Look Newsletter

Since I got involved with the Newsletter redesign last December, I have enjoyed chatting with many people from across the mathematical community about it and about the LMS. In these conversations I have been struck by the warmth, enthusiasm and support of the community toward the LMS. Statements along the lines of "I'd really like to be more involved with the LMS" have come up time and time again. The Society is its members and there are many ways to get more involved with it; you might consider serving on a committee or standing for Council, for instance, and please do take time to vote in the upcoming LMS elections (see page 3).

The Newsletter also provides additional opportunities to get involved, such as the following.

- Feature articles: if you have an idea for a feature article then please consider contributing one. Feature articles should be written for a general mathematical reader, and should be enjoyable to the Society's members as a whole. We consider contributions of feature articles from members and non-members alike, and, of course, contributors need not be UK-based. We especially encourage submissions from early career researchers.
- Micro-theses: micro-theses and nano-theses provide space in the Newsletter for current and recent research students to present their research findings to the wider mathematical community through a one or two page spread. You can find this issue's micro-thesis on page 32. If you are a current or recent research student, consider contributing.
- Ideas: the Newsletter is a community endeavour. If you have some ideas or there is something you'd like to see, please get in touch.

If you are interested in contributing, please see the submission information on the Newsletter's website at newsletter.lms.ac.uk/submissions/.

Finally, I'd like to take the opportunity to thank all those who have contributed to this redesign. Thanks are especially due to the Newsletter Review Committee (Stephen Huggett, Marianne Freiberger, Julia Collins, Richard Elwes, Lucia Di Vizio and Chris Hollings) who set the redesign in motion; Keri Newman for the creation of the Newsletter designs; Sunrise Setting for the creation of the LaTeX class file; as well as the wonderful LMS staff, especially Susan Oakes and Katherine Wright, for their ongoing efforts. The current editorial board also deserves warm thanks. Lastly, on the behalf of the community I'd like to take the opportunity thank the outgoing editor Tony Mann for his contributions to the Newsletter over the years.

Iain Moffatt
Editor-in-Chief

The LMS Mathematical Sciences Directory UK

The London Mathematical Society (LMS) is pleased to announce the official launch of the *LMS Mathematical Sciences Directory*, a comprehensive online resource for and about mathematical scientists in the UK.

Mathematical scientists across the UK in every walk of life – academia, industry, education, commerce, enterprise and beyond – will be able to find and network with potential research collaborators in a single online location.

With the launch of the *MSDirectory*, the LMS seeks to facilitate greater connection, communication and collaboration between mathematical sciences professionals and academics. The *MSDirectory* will exist as a central resource for members of the mathematical community to network within their own discipline and be discovered by colleagues in other sectors.

The advantages of the *MSDirectory* are not exclusive to members of the LMS. Participation is open to anyone who holds, or is registered to study for, a mathematical sciences first degree or above from a UK institution, as well as anyone currently working in mathematical sciences in the UK without such a qualification. It is also open to anyone with a mathematical sciences first degree or above from an overseas institution who now works in the UK.

The *MSDirectory* currently contains the details of over 5,000 UK-based mathematical scientists. As a community strengthening tool, the *MSDirectory* expects to use an active and dynamic membership to grow into the recognised and valued 'home' of mathematical sciences graduates in all career paths.

Privacy and security considerations for *MSDirectory* members are of the utmost importance to the LMS, and careful steps have been taken to protect and secure all stored data as far as possible. Membership of the *MSDirectory* is entirely optional, and it is the choice of the member how much or little of their data is available to view publicly. A member owns and can update their own data at any time.

Members can also choose to remain on the database but not have their data publicly viewable, or to opt out at any point. The LMS Privacy Policy has been updated to disclose how MSDirectory data is obtained, displayed and used: lms.ac.uk/privacy-notice.

It is hoped that *MSDirectory* members will encourage colleagues and collaborators not already listed on the Directory to apply via lms.ac.uk/msd/msd-application-form.

Membership of the *MSDirectory* is entirely separate from membership of the LMS. You do not have to be a member of one to join the other, although Directory members who are not already LMS members are warmly invited to join the Society. The *MSDirectory* exists for all those in the mathematical community in its widest sense.

Ken Brown
LMS Vice-President

LMS Elections 2017

Voting for the LMS 2017 elections for Council and Nominating Committee will open on 5 October 2017.

The slate of candidates can be found at lms.ac.uk/about/council/lms-elections.

An online forum for discussion is available at discussions.lms.ac.uk/elections2017/.

Instructions on how to vote will be sent to members by email or post (depending on recorded preference) before the ballot opens. The election results will be announced at the LMS AGM on 10 November.

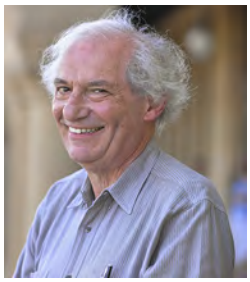
Members are encouraged to ensure that their contact details are up to date (check and edit these at lms.ac.uk/user).

LMS Honorary Members 2017

The LMS elects Persi Diaconis and Étienne Ghys as Honorary Members of the Society.

Persi Diaconis (Mary V. Sunseri Professor of Statistics and Mathematics, Stanford University) is an exceptional mathematician who has made remarkable and wide-ranging contributions to both statistics and mathematics. He is especially known for his results on card shuffling and coin tossing. Diaconis is also a brilliant speaker and an accomplished magician.

Étienne Ghys (Directeur de Recherche CNRS, École Normale Supérieure de Lyon) is a prolific mathematician whose work spans geometry, topology, dynamics, and algebra and who has made important contributions to the theory of foliations and of group actions on circles. Ghys is also a brilliant and multi-faceted expositor of mathematics.



Persi Diaconis (left) and Étienne Ghys (right)

IN BRIEF

Open House 2017

The LMS will for the seventh successive year open its doors to the public as part of this year's Open House London event. De Morgan House will be open on Sunday 17 September from 10 am until 4.30 pm. Visitors will be given a tour of the building and there will also be a presentation on mathematics through the years. Over 350 people visited the building in 2016 and we hope to continue this success in 2017.

Parliamentary Links Day 2017

Representatives from a wide range of STEM organisations, academics, MPs and industrialists gathered for the annual Parliamentary Links Day event in Westminster on 27 June, organised by the Royal Society of Biology (tinyurl.com/ycls7h37).

The audience was welcomed by the Speaker of the House of Commons, the Rt Hon John Bercow MP, and heard keynote presentations from the Minister for Universities and Science, Jo Johnson, and Sir John Kingman, chair designate of UK Research and Innovation (UKRI).

Jo Johnson highlighted the need to address geographical economic imbalances and the willingness of the government to maintain EU collaboration after Brexit. Sir John Kingman stressed that the UKRI is an important strategic objective for government and that it will look to improve oversight across Research Councils and science disciplines.

The presentations were followed by two panel sessions. The first, which included MP Chi Onwurah, Chris Hale from Universities UK, and Professor Roberto Di Lauro and Dr Lorenzo Melchor from (respectively) the Italian and Spanish embassies, looked at *Science and Europe* and discussed scientists' mobility and EU scientists' concerns about taking up positions in the UK. The second, which included Professor Dame Jocelyn Bell Burnell (President, Royal Society of Edinburgh) and Professor Sir John Holman (President, Royal Society of Chemistry), looked at *Science and the World*, in particular the need for specialist scientists in primary schools and better careers advice for students.

The event was followed by a luncheon at the House of Lords, which included an address by Professor Alex Halliday, Vice-President, Royal Society. Professor Halliday's address is available at tinyurl.com/y74994wu.

PEOPLE

2017 David Crighton Medal

I. DAVID ABRAHAMS

The IMA and the LMS have awarded the 2017 David Crighton Medal to Professor I. David Abrahams, Director of the Isaac Newton Institute for the Mathematical Sciences, for his outstanding service to both mathematics and the mathematical community.

David developed the technically demanding Wiener-Hopf techniques for applications in real problems, and created a vibrant group working on waves in Manchester. He has received the Royal Society's Leverhulme Trust Senior Research Fellowship and its Wolfson Research Merit Award.

He has also performed almost all the important roles of a leader in the mathematics community, having sat on and chaired committees for the Research Councils, served on the REF panel twice, and taken senior leadership roles as President of the IMA and Scientific Director at ICMS, in addition to his current role. In all these positions he has supported both the mathematical sciences (in the broadest sense) and mathematical scientists.

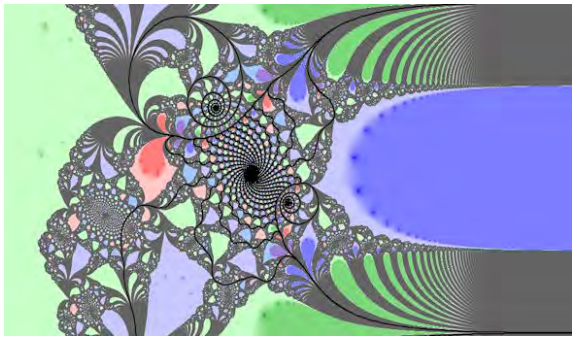
A full citation can be found on the LMS website at tinyurl.com/y9ecsdor. We extend our warmest congratulations to David.

Undergraduate Research Bursary Holders Receive Prestigious Award

LASSE REMPE-GILLEN AND ZHAIMING SHENG

Undergraduate Research Bursary holders Professor Lasse Rempe-Gillen and Zhaiming Sheng of the Department of the Mathematical Sciences at the University of Liverpool have been selected to receive the 2017 Merten M. Hasse Prize from the Mathematical Association of America for their paper, *The Exponential Map is Chaotic: An Invitation to Transcendental Dynamics*. The paper arose from work undertaken during the Undergraduate Research Bursary summer project supported by the London Mathematical Society and Nuffield Foundation in 2013.

The Undergraduate Research Bursary scheme is now run solely by the LMS. The scheme awards grants annually to undergraduates with research experience to help them explore their potential and encourage them to consider a career in scientific research. Since 2013 nearly 150 awards have been made to students at institutions across the UK.



An image that arose from Professor Rempe-Gillen's research on exponential maps

Professor Rempe-Gillen said: "It is a great honour to receive the Merten M. Hasse Prize. We hope that the surprising behaviour of the complex exponential map under iteration will encourage readers to further explore the magic of complex numbers, and the wonders of transcendental dynamics. Undergraduate research projects such as the one that led to this paper are a great opportunity, and I would encourage any undergraduate student interested in research to consider undertaking one. I would also like to gratefully acknowledge support for this work by the Leverhulme Foundation, through a 2012 Philip Leverhulme Prize."

LMS Undergraduate Research Bursaries 2017

The London Mathematical Society is pleased to announce the list of successful applicants to its third round of Undergraduate Research Bursaries. For the 2017 round, 42 awards were made to students from 21 different institutions to undertake a research project alongside a research supervisor. The purpose of the bursaries is to enable undergraduates with research potential to experience research and to encourage them to consider a career in scientific research. The list can be found on the LMS website at lms.ac.uk/bursarylist2017.

REF Main Panel Chairs

The four UK Higher Education Funding Bodies have announced the appointment of the chairs of the four main panels for the Research Excellence Framework (REF) 2021. Main Panel B: Physical sciences, engineering and mathematics will be chaired by Professor David Price, Vice-Provost (Research), University College London. More information about Professor Price is available at ucl.ac.uk/research/vpr.

The Vision for UK Research and Innovation

Professor Sir Mark Walport, Chief Executive Designate of UK Research and Innovation, has given a speech outlining the vision, objectives and next steps in development for the organisation. More information is available at tinyurl.com/ybdz77dq.

Smith Review of Post-16 Mathematics

The London Mathematical Society welcomes the recent report of Professor Sir Adrian Smith's review of post-16 mathematics. As part of the mathematics community, we welcome its recognition of the importance of mathematics, and its analysis of the need to improve take-up and achievement in 16-18 mathematics. The report makes significant recommendations for strengthening the provision of a variety of post-16 mathematics pathways, so that within a decade all 16-18 students should have access to appropriately rewarding and challenging routes of study.

As a society with many members in university mathematics departments, the LMS is pleased by Recommendations 11 and 12. We recognise and support activities that have a positive impact on mathematics attainment in schools and look forward to further support and encouragement from the Department of Education for such work.

The LMS is encouraged by the positive tone of the government response, and hopes that it will be able to work with government and its agencies to further the recommendations of the report. The announcement of funding of £16 million pounds for a new Level 3 Maths Support Programme is a welcome start to implementation of the report's recommendations. However, we are aware that the scale of the issue, including in particular Recommendation 6 on removing disincentives for mathematics provision, and the question of teacher supply, means that there are considerable further funds needed.

The report is available at tinyurl.com/y9cmgvw5 and a response from the Rt Hon Nick Gibb MP, Minister of State for School Standards, is available at tinyurl.com/y7eod8zb.

What Will Maths Education Look Like in 2030?

Professor Frank Kelly, Chair of the Advisory Committee on Mathematics Education (ACME), looks at the need for specialist teachers in schools tinyurl.com/ydyewllp.

New Commons Select Committee Chairs

Newly elected committee chairs for the new Parliament have been announced by the Speaker, the Rt Hon Sir John Bercow. Committees of interest are listed below.

- Business, Energy and Industrial Strategy: Rachel Reeves (Labour)
- Education: Robert Halfon (Conservative)
- Science and Technology: Norman Lamb (Liberal Democrat)

Information on all newly elected chairs is available at tinyurl.com/yas3f9o6.

John Johnston
Joint Promotion of Mathematics

EUROPEAN

Jean-Pierre Kahane

Professor Jean-Pierre Kahane, past president of the *Société Mathématique de France*, and specialist in harmonic analysis and probability, passed away on 21 June 2017 at the age of 90. Many tributes to the life and mathematics of Professor Kahane, including the message read by Cedric Villani at the funeral ceremony on 30 June, can be found at smf.emath.fr/content/décès-jean-pierre-kahane.

CIEM 2018

The CIEM (*International Center for Mathematical Meetings*) is an initiative of the University of Cantabria, Spain whose goal is to promote quality mathematical research, be it in its more basic or its more applied and computational aspects, with special emphasis on multidisciplinary ventures. It has organized 130 events since its foundation in 2006.

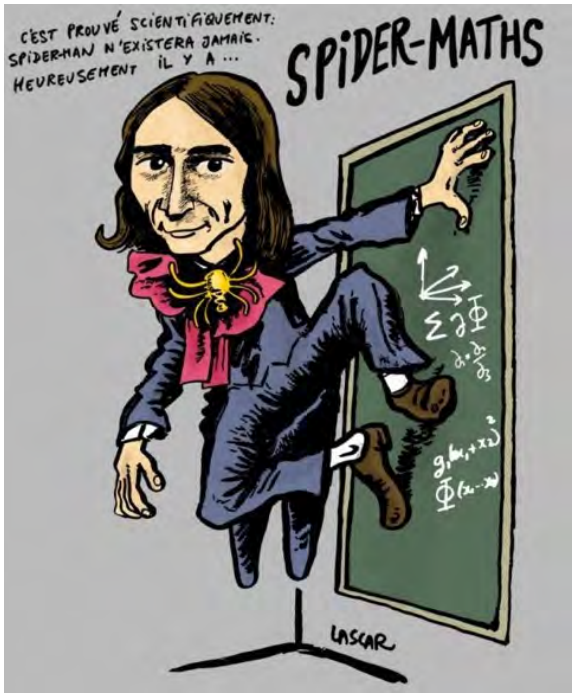
The CIEM is now seeking activity proposals for the year 2018. Individuals and groups interested in organizing a workshop, meeting, advanced course, etc. are invited to ask for the CIEM to allocate that event in its annual program. The candidate events must be thematically related to mathematics or close fields (computer science, theoretical physics,..) and their quality be guaranteed by a scientific and/or organizing committee. Their length should preferably be one week (Monday to Friday), but three-day meetings and, exceptionally, two-week meetings are also allowed.

The CIEM offers its resources (lecture room for 100 people, smaller meeting rooms, internet Wi-Fi, computer room, etc.) plus logistic and monetary support for the organization, accommodation, etc.

Proposals should be sent by email to ciem@unican.es preferably before **10 September 2017**. The application letter should contain a brief description of the event, previous similar meetings if any, organizing committee, expected number of attendees, expected external financing, financial support asked from CIEM, and any other information that supports the quality and feasibility.

Additional information is at ciem.unican.es.

Cédric Villani as seen by Le Canard Enchaîné



David Chillingworth
LMS/EMS Correspondent

OPPORTUNITIES

William Hodge Fellowships at IHES

The William Hodge Fellowships offer two young researchers in mathematics or theoretical physics a one or two year postdoctoral position at the Institut des Hautes Études Scientifiques (IHES), France.

The fellowship, named after Sir William Hodge, the eminent British mathematician, LMS President 1947-49, was created in 2001 in partnership with the EPSRC that has been supporting the IHES for many years in order to develop links between the British and French research institutions. It encourages British mathematicians and theoretical physicists to apply to IHES.

The next call for applications to the IHES Hodge Fellowship programme is autumn 2017. The selection of successful candidates will take place in December 2017. For more information visit the IHES website ihes.fr.

VISITS

Visit of Raffaele Vitolo

Professor Raffaele Vitolo (University of Salento, Lecce, Italy) will be visiting the UK between 12 and 26 November 2017. Professor Vitolo works on Hamiltonian formalism and integrable systems. Provisional details of Professor Vitolo's talks during his visit are:

- University of Glasgow, 16 November (contact Ian Strachan: Ian.Strachan@glasgow.ac.uk)
- University of Leeds, 17 November (contact Allan Fordy: A.P.Fordy@leeds.ac.uk)
- Loughborough University, 22 November (contact Jenya Ferapontov: E.V.Ferapontov@lboro.ac.uk)

For further details contact Jenya Ferapontov. The visit is supported by an LMS Scheme 2 grant.

Visit of Henrik Holm

Dr Henrik Holm will visit Newcastle University from 20 to 26 November 2017 on an LMS Scheme 4 grant. He will give a lecture on quiver representations and model category structures on Tuesday 21 November. Dr Holm has been based at the University of Copenhagen since 2012. He is a leading expert on Gorenstein homological algebra whose paper *Gorenstein homological dimensions* from 2004 has more than 250 citations. His current research concerns abelian categories of quiver representations, with a particular view to the construction of model category structures.

For information regarding Dr Holm's visit, contact Peter Jorgensen at the School of Mathematics at Newcastle University (peter.jorgensen@ncl.ac.uk).

Visit of Daniil Proskurin

Dr Daniil Proskurin (Taras Shevchenko National University of Kiev, Ukraine) will be visiting the UK between 5 and 18 November 2017. His main research interests are in operator algebras, in particular, C*-algebras and their representations. Details of Dr Proskurin's talks during his visit are:

- Swansea University, 9 November (contact Eugene Lytvynov: e.lytvynov@swansea.ac.uk)
- University of Sheffield, 15 November (contact Vladimir Bavula: v.bavula@sheffield.ac.uk)
- University of York, 16 November (contact Alexei Daletskii: alex.daletskii@york.ac.uk)

For further details contact Eugene Lytvynov. The visit is supported by an LMS Scheme 2 grant.

UNIVERSITY OF CAMBRIDGE

ADAMS PRIZE

The Mathematics of Astronomy and Cosmology

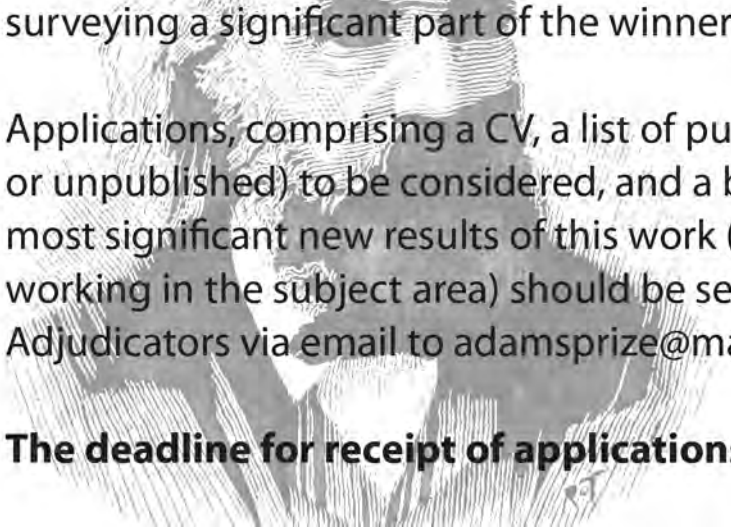
The University of Cambridge has announced the subject for one of its oldest and most prestigious prizes. The Adams Prize is named after the mathematician John Couch Adams and was endowed by members of St John's College. It commemorates Adams's role in the discovery of the planet Neptune, through calculation of the discrepancies in the orbit of Uranus.

The Chairman of the Adjudicators for the Adams Prize invites applications for the 2017-18 prize which will be awarded this year for achievements in the field of The Mathematics of Astronomy and Cosmology.

The prize is open to any person who, on 31st October 2017, will hold an appointment in the UK, either in a university or in some other institution; and who is under 40 (in exceptional circumstances the Adjudicators may relax this age limit). The value of the prize is expected to be approximately £15,000, of which one third is awarded to the prize-winner on announcement of the prize, one third is provided to the prize-winner's institution (for research expenses of the prize-winner) and one third is awarded to the prize-winner on acceptance for publication in an internationally recognised journal of a substantial (normally at least 25 printed pages) original article, of which the prize-winner is an author, surveying a significant part of the winner's field.

Applications, comprising a CV, a list of publications, the body of work (published or unpublished) to be considered, and a brief non-technical summary of the most significant new results of this work (designed for mathematicians not working in the subject area) should be sent to the Secretary of the Adams Prize Adjudicators via email to adamsprize@maths.cam.ac.uk.

The deadline for receipt of applications is 31st October 2017.



LMS Women in Mathematics and Girls in Mathematics events 2017–18

The London Mathematical Society is inviting expressions of interest in hosting a Women in Mathematics or Girls in Mathematics event in 2017-18.

Women in Mathematics

The Women in Mathematics Committee is inviting individuals or groups to express interest in organising and hosting a Women in Mathematics Day in academic year 2017–2018. These events are aimed at academic mathematicians (from at least postgraduate level and up and may include undergraduates). The events are intended to help early career women mathematicians when considering the next stages in their careers and typically have included mathematical talks combined with panel discussions, social opportunities and networking. For details of previous events organised by the Society visit the website at lms.ac.uk/events/previous-women-mathematics-days.

Funding is available for one event in academic year 2017–18. Up to **£3,000** of funding is available for the event. Details on how to submit an expression of interest can be found at http://tinyurl.com/y6ub43tc.

Girls in Mathematics

The Women in Mathematics Committee is inviting individuals or groups to express interest in organising a Girls in Mathematics event in academic year 2017–18. Events should be aimed at schoolgirls, up to and including A-levels or equivalent, with mathematics as a main focus.

Funding is available for two events in the academic year 2017-18. Up to **£500** of funding is available for each event. Details on how to submit an expression of interest can be found at http://tinyurl.com/y6ub43tc.

LMS Council Diary: a Personal View

At the meeting of Council on the 30 June 2017, the President updated Council on activities undertaken since the most recent meeting, including attending Council's visit to the New Mathematics Gallery at the Science Museum. The President Designate provided an update on the workings of the Strategic Sub-Group, which has been discussing the Society's governance arrangements with regards to the practical workings of Council. As an interim measure prior to any significant changes being discussed, the President Designate proposed that Council consider reducing its meetings to five per year, and reducing F&GPC meetings to four per year; Council agreed to trial this new arrangement in 2018.

The Treasurer introduced the Third-Quarter financial review for 2016–17, beginning by informing Council that it was expected there would be a large surplus at year-end instead of the previously forecast slight deficit. This alteration was largely due to devaluation of the pound against the US dollar, which affected international trade in Publications. The Treasurer also noted that Wiley had sold a larger number of licencing deals than forecast, and that the De Morgan House Conference Facilities income had also increased. It was noted that the Society had underspent in an unusually high number of areas, though in part this is due to timing, with some further funds to be spent by year-end.

The Treasurer then presented Council with proposed budgets for 2017–18 and planning figures for 2018–20. Again, the devaluation of the pound against the US dollar had caused some changes in the circumstances, with the Society's investment portfolio having significantly increased as a result. It was forecast that there would be a surplus in each of the next three years, and some possibilities for use of surplus funds were discussed. The Treasurer also reported

on the Investment Sub-Committee's meeting held on 12 June 2017; Sub-Committee had discussed the Society's portfolio of investment property.

Vice-President Brown then provided an update on Research Policy Committee matters. One item of note was that the Deputy Chief Executive of the Engineering and Physical Sciences Research Council (EPSRC) had contacted the Chair of the Council for Mathematical Sciences (CMS) with regards to the mathematical sciences' lack of access to the Global Challenges Research Fund. EPSRC had offered £40k funding to the CMS to organise a meeting that would be used to inform the focus of future funding calls. The CMS had accepted the offer and was discussing the arrangements for such a meeting in partnership with the Isaac Newton Institute and the International Centre for Mathematical Sciences.

Tara Brendle

LMS Grant Schemes

For full details of the following grant schemes, and for information on how to make an application, please visit lms.ac.uk/grants.

Schemes 1–5 (Research Grant Committee)

The following grant schemes are offered by the LMS Research Grants Committee. The deadline for grant applications under Schemes 1–5 is **15 September 2017**.

Scheme 1: Conference Grants
Grants are made to the organisers of conferences to be held in the UK. Priority is given to the support of meetings where an LMS grant can be expected to make a significant contribution to the viability and success of the meeting. Support of larger meetings of high quality is not ruled out, but for such meetings an LMS grant will normally cover only a modest part of the total cost.

Scheme 2: Visitors to the UK
Scheme 2 aims to provide grants to mathematicians based within the UK to partially support visitors to the UK; the visitors are expected to give lectures in at least three separate institutions.

Scheme 3: Support of Joint Research Groups
Scheme 3 aims to provide support for groups of mathematicians, working in at least three different locations (of which at least two must be in the UK), who have a common research interest and who wish to engage in collaborative activities. It is expected that four meetings will be held in the academic year (or an equivalent level of activity).

Scheme 4: Research in Pairs
Scheme 4 aims to provide small grants to mathematicians within the UK to help support visits for collaborative research.

Scheme 5: International Short Visits
Scheme 5 is intended to provide grants to mathematicians within the UK to support visits for collaborative research, either to or from a country in which mathematics is considered to be in a state of development.

Scheme 7 (Computer Science Committee)

This scheme is offered by the LMS Computer Science Committee; the deadline for submission of applications is **1 October 2017**. The scheme aims to provide support for visits to undertake collaborative research at the interface of Mathematics and Computer Science.

Schemes 8 & 9 (Early Career Research Committee)

The following schemes are offered by the LMS Early Career Research Committee; the deadline for submission of applications is **15 October 2017**.

Scheme 8: Postgraduate Research Conferences
The aim of this Scheme is to support postgraduate research conferences, organised by and for postgraduate research students, to be held in the UK.

Scheme 9: Celebrating New Appointments
Grants are made to provide partial support for meetings held in the UK to celebrate the appointment of a new lecturer in mathematics at a UK institution. The aim of the grant award is to embed the new lecturer in their home institution and the local mathematical community, and to allow the new appointment to create useful and lasting relationships with the local mathematical community. It is expected that the new appointment themselves will present a lecture at the meeting.

Annual LMS Subscription 2017–18

Members are reminded that their annual subscription, including payment for additional subscriptions, for the period November 2017-October 2018 is due **on 1 November 2017 and payment should be received by 1 December 2017**. Please note that payments received after this date may result in a delay in journal subscriptions being renewed.

LMS membership subscription rates 2017–18

Ordinary membership	£80.00	US$160.00
Reciprocity	£40.00	US$80.00
Career break or part-time working	£20.00	US$40.00
Associate membership	£20.00	US$40.00

Access to LMS Journals

The Society offers free online access to the *Bulletin, Journal* and *Proceedings of the London Mathematical Society* (provided by Wiley) and to *Nonlinearity* (provided by the Institute of Physics) for personal use only. If you would like to receive free electronic access to these journals, please indicate your choices either on your online membership record under the "Journal Subscription" tab or on the LMS subscription form. The relevant publisher will then contact members with further details about their subscription.

Subscribing to the EMS and JEMS via the LMS

Members also have the option to pay their European Mathematical Society subscription via the LMS and subscribe to the Journal of the EMS: If you would like to subscribe to the EMS and JEMS via the LMS, please indicate either on your online membership record under the "Journal Subscription" tab or on the LMS subscription form.

Payment of membership fees for EWM

LMS members who are also members of European Women in Mathematics may pay for their EWM fees when renewing their LMS membership. You decide yourself your category of fees: high, normal, low. Please indicate your category of fee either on your online membership record under the "Journal Subscription" tab or on the LMS subscription form. To join EWM please register first at tinyurl.com/y9ffpl73. Please note it is not possible to join the EWM through the LMS.

Online renewal and payment

Members can log on to their LMS user account (lms.ac.uk/user) and make changes to their contact details and journal subscriptions under the "My LMS Membership" tab. Members can also renew their subscription by completing the subscription form and including a cheque either in GBP or USD. We regret that we do not accept payment by cheques in Euros.

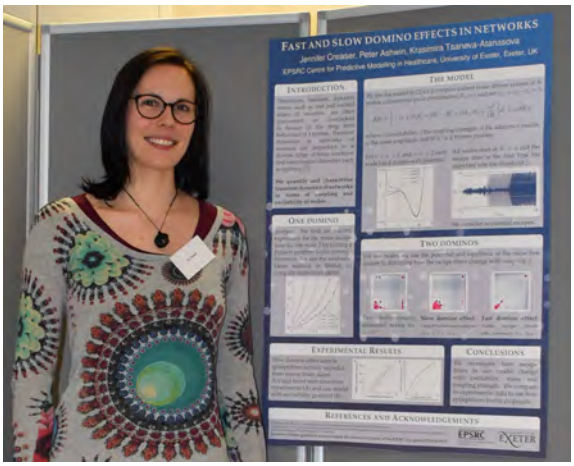
LMS member benefits

Members are reminded that their annual subscription entitles them to the following range of benefits: Voting in the LMS Elections, free online access to selected journals, the newly revamped bi-monthly Newsletter, use of the Verblunsky Members' Room at De Morgan House in Russell Square, London and use of the Society's Library at UCL, among others. (For a full list of member benefits, see lms.ac.uk/membership/member-benefits).

Elizabeth Fisher
Membership Engagement Officer
membership@lms.ac.uk

REPORTS OF THE LMS

Report: Women in Mathematics Day



Poster prize winner Jen Creaser

Birkbeck, University of London organised a two-day Women in Mathematics Conference, from 29 to 31 March 2017, supported by the LMS and Winton. The first day (*Winton Women Trailblazers in Mathematics*) saw school students from underprivileged schools across London learn more about mathematics and the range of careers that use it. Female mathematicians delivered talks demonstrating the presence of maths in a range of unexpected places and there were mathematical challenges for students.

The second day was the *LMS Women in Mathematics Day*, aimed at women from undergraduate level upwards. Eva Kaufholz opened the day with a historical talk about women mathematicians, followed by Caroline Colijn, who talked about the interface between mathematics and biology.

Over lunch there was a poster session featuring posters by PhD students and postdocs. After the poster session we heard three short talks by PhD students.

Ulrica Wilson opened the afternoon, describing her research on eventual properties of matrices. Ruth Kaufman ended the day talking about the huge range of problems that can be tackled under the term "operational research". The day finished with a reception and presentation of the best poster prize to Jen Creaser.

We're grateful to Winton for hosting the conference and to the LMS for its generous funding.

Sarah Hart (Birkbeck)
Conference Organiser

CORRECTIONS AND CLARIFICATIONS

From the July issue (471) of the *Newsletter*.
Page 11: 11 June rather than 11 July.
Page 11 footnote: $12^3 + 1^3 = 10^3 + 9^3 = 1729$.
Page 20: wrongly captioned Dominic Joyce as Simon Donaldson.

W.T. Tutte (1917–2002): Codebreaker–Mathematican

BÉLA BOLLOBÁS

Abstract. This year is the centenary of the birth of Bill Tutte. Tutte is something of an unsung hero: he was perhaps the greatest codebreaker of World War Two, and after the war his mathematical research shaped whole areas of mathematics.

Bronze bust of W.T. Tutte by G. Bollobás, 1977.

William Thomas ("Bill") Tutte was born in Newmarket on 14th May, 1917. At the time his father, William John Tutte, a jobbing gardener, and his mother, Annie Newell, a cook and housekeeper, were working in Fitzroy House, a horse racing stable. The depression that followed WWI hit his parents hard, so young Bill lived in four different places before he turned six. At this time they returned to the Newmarket area, so that his father could work in the Rutland Arms Hotel. At eleven, Bill won a scholarship to the Cambridge and County School for Boys (no mean achievement!), where his interest in mathematics was awakened by W.W. Rouse Ball's *Mathematical Recreations and Essays*. Encouraged by his headmaster, he applied to Trinity College, Cambridge: his application was successful, and in 1935 he went up to Cambridge to read Natural Sciences, specializing in chemistry.

In Trinity College Tutte struck up a life-long friendship with three of his contemporaries: Leonard Brooks, Cedric Smith and Arthur Stone. It soon became apparent that Tutte, the chemist, was even more of a mathematician than his friends. With characteristic modesty, as they wrote later, the four students called themselves the *Important Members* of the Trinity Mathematical Society or, simply, *The Four*. They had so much fun with mathematics that they even created a mathematical poetess, Blanche Descartes, in whose name they published papers, problems and solutions for several decades.

The Four became interested in an unusual question Paul Erdős had brought to England the year before: 'Can a square be tiled by finitely many squares of different sizes?' Briefly: 'Is there a PSS, a Perfect Squared Square?' (The similarity to Max Dehn's theorem about tiling a rectangle with squares is only superficial.) Unbeknown to The Four, this beautiful question of recreational mathematics had been looked at by many people, including the distinguished Russian analyst, Nikolai Luzin, who claimed, but did not prove, that there was no PSS. The Important Members worked on this problem for three years. After many failed attempts, they established a connection between PSSs and currents in an electrical network satisfying Kirchhoff's laws, and found a PSS of order 69 (that is a PSS made up of 69 small squares). Curiously, a few months before the publication of this result, Roland Sprague, a mathematician in Berlin, had published a PSS of order 55 that he found empirically.

This ingenious bit of mathematics of The Four had momentous consequences. When WWII broke out, Tutte was summoned to his tutor, Patrick Duff, and was told to go to Bletchley Park for an interview for a war job. Following this interview and a few weeks in London in a cryptographic school, Tutte joined the small but elite Research Section of the Government Code and Cypher School at Bletchley Park, the forerunner of GCHQ in Cheltenham.

It is widely known that the cryptographers at Bletchley Park, led by Alan Turing, were very successful with the German machine-cipher called *Enigma*. Much less is known about Tutte's role in breaking the incomparably harder and much more important machine-cipher *Tunny*.

In the early 1930s the French, and later the British, obtained from a spy an operating manual and two sheets of monthly key settings for the three-wheeled Enigma machine, and they also acquired a commercial machine. In spite of this, they were unable to decipher secret German messages. However, when they passed all this information to Polish Intelligence, three young Polish mathematicians in Pozna, Jerzy Rozycki, Henryk Zygalski and Marian Rejewski, managed to work out the internal wiring of the German military machine, and even built an electromechanical device to help deciphering messages. When Germany overran Poland, the Polish codebreakers tremendously surprised their French and British counterparts when they gave them copies of the German military Enigma machine, and passed on everything that they had discovered. All this was only the beginning: the codebreakers at Bletchley Park had to keep up with the modifications the Germans kept introducing: they had to break the codes *fast* for the results to be of any use. To achieve this, Turing designed a 'bombe', an electromechanical device much beyond what the Poles had built. By the end of the war, about two hundred bombes had been built to keep up with the flow of messages. Although the Enigma used by the German Army remained recalcitrant, the cryptanalysts at Bletchley Park were experts at breaking Navy and Air Force Enigma messages.

Enigma used Morse code and was for low-level communications. In addition to Morse code, from 1941 the Germans used radio links: at Bletchley this non-Morse traffic became known as *Fish*. As with Enigma, Fish came in three flavours: Army, Air Force and Navy. Although nobody at Bletchley Park had any idea what machines produced Fish, the codebreakers were determined to break the code used by the Army, which they named *Tunny*. This was a high-level cipher used between generals in the field and their command centres; many of the messages were signed 'Adolf Hitler, Führer'.

The cipher messages were in the 5-bit 32-letter Baudot Teleprinter Code alphabet, and were produced by the Lorenz 40/42 teleprinter cipher attachment. Each encrypted message of Tunny started with a sequence of twelve letters, occasionally even expanded into common personal names like Anton, Bertha, etc. It was assumed that these twelve letters specified the settings of twelve wheels.

The codebreakers were helped by a serendipitous event on 30th August 1941, when a long message from Athens to Vienna could not be read clearly by the recipient, and the German operator resent the

Graph theory: factors, cycles and connectivity

A *1-factor* of a graph on n vertices is a set of $n/2$ edges that is incident with all vertices. Trivially, an odd component (i.e., one with an odd number of vertices) cannot have a 1-factor.

Theorem 1. *A graph G with vertex set V has a 1-factor if and only if for any set $U \subseteq V$ the graph $G - U$ has at most $|U|$ odd components.*

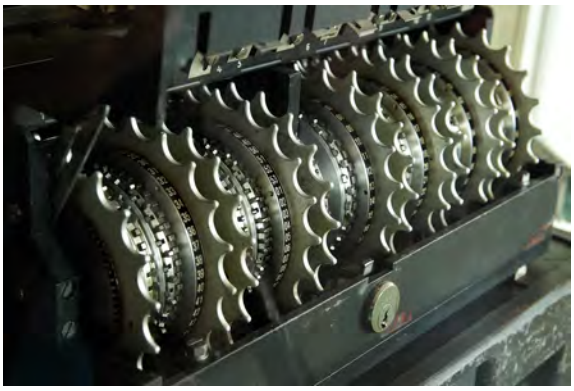
A graph is *cyclically k-edge-connected* if the deletion of fewer than k edges cannot create two components containing cycles. Also, a graph is *k-vertex-connected* or just *k-connected* if the deletion of fewer than k vertices cannot disconnect the graph. In 1884, P.G. Tait made the conjecture that every cyclically 3-edge-connected planar cubic graph has a Hamilton cycle. This conjecture is easily seen to imply the Four Colour Conjecture. In 1946, Tutte disproved Tait's conjecture; later he showed that a stronger condition on the connectivity of the graph does imply the existence of a Hamilton cycle.

Theorem 2. *There is a cyclically 3-edge-connected planar cubic graph on 43 vertices that does not have a Hamilton cycle.*

Theorem 3. *Every 4-connected planar graph is Hamiltonian.*

It seems to be difficult to give structural characterizations of highly connected graphs. In 1961, Tutte gave such a characterization of 3-connected graphs. The building blocks of this characterization are the *wheels*, graphs obtained from a cycle by adding a vertex and all the edges joining this vertex to the vertices of the cycle.

Theorem 4. *A graph is 3-connected if and only if it can be obtained from a wheel by repeated applications of the following two operations.*
(i) *Addition of an edge.*
(ii) *'Splitting' of a vertex x with at least four neighbours, $x_1, \ldots, x_k$, $k \geq 4$, i.e. replacing x by two vertices, x', x'', and joining each x_i to at least one of them, making sure that each of x' and x'' is joined to at least three of the x_i.*



The wheels of a Lorenz machine. (Photo courtesy of The National Museum of Computing www.tnmoc.org.)

message with the same wheel settings but with slightly different punctuation and word-spaces. This enabled the veteran cryptanalyst Brigadier John Tiltman to work out a piece of the Tunny key. In spite of this lucky break, all the might of the cryptographers at Bletchley Park got nowhere with breaking the Tunny code, i.e. with describing a machine that could produce such a key. In October 1941 Tutte was given the Tunny key and the associated documents: "See what you can make of this". After a few months of deep thinking, Tutte broke the back of the problem. As he wrote many years later: "At this stage the rest of the Research Section joined in the attack. . . . Thus were the entire workings of the Tunny machine exposed without any actual physical machine or manual thereof coming into our hands."

Not surprisingly, the messages they managed to decode were too old to be of any interest. It was imperative to use Tutte's discoveries *fast*, so the computations had to be done mechanically. This mechanization was carried out by the technical genius Tommy Flowers, who built the pioneering electronic computer *Colossus* for this purpose. Soon coded messages could be broken in 24 hours, and were passed on to the military as *"Ultra"* intelligence. By the end of the War, ten Colossus machines were working on Tunny codes.

Bill Tutte and Tommy Flowers are the two unsung heroes of WWII. Breaking Tunny is often called the single greatest intellectual feat of WWII: it remained extremely important to the end of the war. In particular, "Ultra" messages were vital in the decisive battle of Kursk, and in the weeks leading up to D-Day. The official historian of British Intelligence, Harry Hinsley, wrote that the "Ultra" intelligence produced at Bletchley Park shortened the war by two to four years, and that without it the very outcome of the war would have been uncertain.

Sadly for Tutte and Flowers, their achievements were Official Secrets for far too long, and as a result they received far too little recognition for their war work. It seems that almost all the accolades go to Alan Turing, who was indeed a great mathematician – a host of books, a beautiful bust at Bletchley Park, and even a Hollywood film sing his praise.

To the credit of Tutte's superiors at Bletchley Park, in the fall of 1942 they paid a visit to J.E. Littlewood, the great analyst and an important Fellow of Trinity College, to tell him that Bill Tutte *must* be given a Prize Fellowship for his War work. They would not say a word about what Tutte had done, only that he must be elected. So in October 1942 Littlewood told the Electors that Tutte must be given a Fellowship for his secret work, and Tutte duly became a Fellow of Trinity College. Nevertheless, Tutte remained at Bletchley Park till the end of the war, when he returned to Cambridge to take up his Fellowship in Trinity College.

As Tutte could not submit his codebreaking results in a Ph.D. dissertation, he returned to his old love, graphs. Working independently of his supervisor, Shaun Wylie, who had also returned to Cambridge from Bletchley Park, he wrote an outstanding and exceptionally long dissertation on algebra and graph theory, and, especially, the combination of the two. After he received his Ph.D. in 1948, he accepted a position in Toronto at the invitation of the great geometer Donald Coxeter (a former Research Fellow of Trinity College). A year later he married Dorothea Mitchell, and in 1962 he moved to the University of Waterloo (founded in 1958), officially retiring in 1982. Bill and Dorothea did not live in Waterloo, but in the tiny village of West Montrose, just over ten miles from the campus. Their house was near a local landmark, a covered bridge (the only one in Ontario): they enjoyed their beautiful garden, went for long hikes and canoed on the river.

Tutte was not only a phenomenal codebreaker, but also a great mathematician. (The boxes in this article contain nine beautiful results of Tutte that can be stated easily.) Today combinatorics is a flourishing and dynamic branch of mathematics, attracting many of the most talented young mathematicians, but in the 1940s and later it was considered to be a very low class area of mathematics. That bit by bit the fortunes of combinatorics changed over the years is due mostly to two giants: Paul Erdős, a frequent

visitor to Cambridge for fifty years, and Bill Tutte. Erdős championed extremal and probabilistic combinatorics, while Tutte developed structural graph theory in conjunction with algebra, proving great results on Hamilton cycles, factors of graphs, colourings, maps, and highly connected graphs. Tutte's work on the foundation of matroid theory, building on results in his dissertation, his numerous deep results on structural graph theory, the introduction of the Tutte polynomial, and his deep work over three decades on enumerating various classes of planar maps had a profound influence on mathematics going beyond combinatorics. I shall say a few words about these achievements.

Enumeration of maps

A planar map is a connected graph (with loops and multiple edges allowed) drawn on the sphere, with two embeddings considered to be identical if they are ambient isotopic. To attack the problem of counting the number of planar maps within reach, Tutte considered 'rooted maps', maps with a fixed oriented edge with a marked side—the point being that rooting a map destroys its symmetries.

Theorem 5. *The number a_n of rooted maps with n edges is*

$$a_n = \frac{2\cdot(2n)!}{n!(n+2)!}\,3^n \sim \frac{2}{\sqrt{\pi}}\,n^{-5/2}12^n,$$

and the number b_n of 2-connected maps with n edges is

$$b_n = \frac{2(3n-3)!}{n!(2n-1)!} \sim \frac{2}{9(3\pi)^{1/2}}\,n^{-5/2}\left(\frac{27}{4}\right)^n.$$

Theorem 6. *The number of rooted bipartite planar maps with n vertices, m edges and f faces, f_k of which have degree $2k$, is*

$$\frac{2\cdot m!}{(m-n+2)!}\prod_{k\geq 1}\binom{2k-1}{k}\frac{1}{f_k!}.$$

Remarkably, the exponent $-5/2$ appearing in the formulae in Theorem 5 is conjectured to be universal for a wide class of maps.

Although nowadays we view Tutte's work as the continuation of earlier results, he made his discoveries independently of earlier work, discovering whatever he needed. Thus, for his Ph.D. dissertation, among other topics, he investigated *"nets"*, which later turned out to be equivalent to *representable matroids*.

In his free time at Bletchley Park, Tutte thought much about Hamilton cycles in graphs. In 1884, P.G. Tait, best known for his conjectures in knot theory, made the conjecture that every cyclically 3-connected planar cubic graph is Hamiltonian. If true, this conjecture would have implied the Four Colour Theorem. Building on a graph in which there is an edge that is in every Hamilton cycle, Tutte constructed a counterexample. In his dissertation he used *"cleavages"* to find 3-connected parts of a 2-connected graph, and gave a structural characterization of 3-connected graphs. Later he extended a result of Whitney to deduce that every 4-connected planar graph is Hamiltonian.

Tutte also proved major results about factors of graphs, enumeration of triangulations and planar maps, and the notorious (and still unsolved) Reconstruction Conjecture of Ulam.

Matroids were introduced by Hassler Whitney in 1935 as abstractions of the notion of linear independence among sets of vectors, and further contributions were made by Garrett Birkhoff, S. MacLane and B.L. van der Waerden. Nevertheless, the foundation of matroid theory is mostly due to Tutte, who in his 1948 thesis made the first real advances in the theory. In particular, he proved major results about matroids with excluded minors, characterizing binary matroids, regular matroids and graphic regular matroids.

Many years later, Tutte's work on minors was extended by Robertson and Seymour in a great series of papers with many deep results, including the Graph Minor Theorem that every infinite set of finite graphs contains two graphs with one a minor of the other.

In a paper published in 1947 and then in his thesis, Tutte introduced a polynomial he called the *dichromatic polynomial*. (In fact, the germs of this polynomial go back to the work of The Four on PSS.) This polynomial, which is now known as the *Tutte polynomial*, may well be Tutte's most important contribution to mathematics. It is a two-variable extension of the chromatic polynomial introduced by G.D. Birkhoff some decades earlier. The versatility of this polynomial and its descendants is astounding: it has important applications not only in graph theory and matroid theory, but also in statistical mechanics, percolation theory, coding theory and knot theory. Thus, the *Jones polynomial*, introduced almost forty years later, is a 'coloured' Tutte polynomial, and the Jones

polynomial of alternating knots is just a univariate specialisation the Tutte polynomial. By now there are a host of extensions of the Tutte polynomial, and its evaluations are still being discovered to count more and more interesting structures.

Tutte wrote several series of papers on the enumeration of planar maps: on the 'census of maps' in the early 1960s, on 'chromatic sums' in the early 1970s, and on functional equations related to these a decade later, returning to all another decade later. The starting point was the enumeration of classes of planar maps, i.e. connected multigraphs with loops embedded in the sphere, up to continuous deformations.

The Tutte polynomial

Although in extremal graph theory we tend to study graphs without multiple edges and loops, when it comes to polynomials on graphs, the natural domain is the set $\mathcal{G}$ of graphs with multiple edges and multiple loops allowed. In defining his polynomial, Tutte made use of two graphs derived from a graph G: deleting ('cutting') an edge e we get $G - e$, and contracting ('fusing') e, the graph G/e. Thus G/e is obtained by identifying the vertices of e, and deleting the loop that e becomes. Special roles are played by loops and bridges, edges whose deletion increases the number of components.

Theorem 7. *There is a unique map $T : \mathcal{G} \to \mathbb{Z}[x, y]$, $G \mapsto T_G(x, y)$, such that*

$$T_G = \begin{cases} xT_{G/e} & \text{if } e \text{ is a bridge,} \\ yT_{G-e} & \text{if } e \text{ is a loop,} \\ T_{G/e} + T_{G-e} & \text{if } e \text{ is an ordinary edge,} \end{cases}$$

and if G has no edge then $T_G = 1$.

The *Tutte polynomial* is the unique polynomial $T_G(x, y)$ in this theorem. In fact, Tutte's interest in recursive formulae based on the cut and fuse operations was awakened in his undergraduate days, when The Four applied these operations to electrical networks.

Tutte also gave several explicit formulae for T_G: here is one of them. For a graph $G = (V, E)$ with a set V of n vertices, a set E of m edges and k components, the rank of G is $r(G) = n - k$ and its nullity is $n(G) = m - n + k$. For $F \subseteq E$, the graph (V, F) is denoted by $\langle F \rangle$.

Theorem 8. *The Tutte polynomial of a graph $G = (V, E)$ is*

$$T_G(x, y) = \sum_{F \subseteq E} (x - 1)^{r(G) - r\langle F \rangle} (y - 1)^{n\langle F \rangle}.$$

Here is a selection of evaluations of the Tutte polynomial counting interesting combinatorial structures.

Theorem 9. *Let G be a connected graph. Then*

(i) $T_G(1, 1)$ *is the number of spanning trees;*

(ii) $T_G(2, 1)$ *is the number of spanning forests;*

(iii) $T_G(1, 2)$ *is the number of connected spanning subgraphs;*

(iv) $T_G(2, 2)$ *is the number of spanning subgraphs, i.e. 2^m, where m is the number of edges;*

(v) $T_G(2, 0)$ *is the number of acyclic orientations of G, i.e. the number of ways to direct its edges so that there are no directed cycles;*

(vi) $T_G(1, 0)$ *is the number of acyclic orientations of G with a fixed vertex u as the only source, provided G is connected;*

(vii) $T_G(0, -2)$ *is the number of ice configurations of a 4-regular graph G, i.e. orientations of the edges in which each vertex has indegree 2 and outdegree 2.*

To get a handle on this problem, Tutte considered *rooted* maps, maps with a distinguished oriented edge with a marked side. For example, he showed that the number of rooted planar maps with n edges is $\frac{2(2n)!}{n!(n+2)!}\ 3^n$. In the 'chromatic sums' series, he studied the generating functions for maps indexed by several invariants, weighted by their chromatic or Tutte polynomials.

The significance of this area has been recognized only in the last two decades: now we know that Tutte's results have deep connections to random surfaces, quantum gravity, the Ising model of random triangulations, and other important fields.

Dorothea and Bill: Birthday Banquet, Trinity College, Cambridge, 14th May, 1977.

Outside combinatorics, Tutte is still greatly underestimated: he became an FRS decades late, only after he had retired from Waterloo, and was never awarded a knighthood, let alone the peerage he so richly deserved. Canada was kinder to him: in 1958 he was made an FRSC, and in 2001 he became an Officer of the Order of Canada. He was touched that in 1977 I organized an international conference for his 60th birthday in his beloved Trinity College, at which The Four were reunited and his old tutor presided over the Birthday Banquet. Forty years later the *Tutte Centenary Conference* has just taken place in Trinity College, at which outstanding speakers paid tribute to Tutte's work and presented important developments that arose from it.

Dorothea, without whom one could not imagine Bill, died in 1994, and a couple of years later Bill moved back to England. Sadly, he did not settle in Cambridge, where he would have found a stimulating environment in his beloved Trinity College, with regular high-level combinatorics seminars in the Centre for Mathematical Sciences, and many visiting mathematicians, but returned to Newmarket. Some years later he moved back to Waterloo, where on 2nd May 2002 he succumbed to congestive heart failure, complicated by lymphoma of the spleen.

Tutte's contribution to the war, and thereby our lives, is hard to overstate and had just begun to be recognised. In particular, in 2012 the then Prime Minister David Cameron wrote a letter of thanks to his niece, Mrs Jeanne Youlden. The sentiments expressed in this letter are a fitting tribute to Bill Tutte.

> "I am writing to you to express my personal thanks and the United Kingdom's gratitude for the work of Professor William 'Bill' Tutte.
>
> The success of cryptographers at Bletchley Park was an iconic British triumph of the Second World War and their achievements represent one of history's greatest intelligence successes."

Béla Bollobás

Béla Bollobás received a doctorate in Budapest, and another in Cambridge, where he has been a Fellow of Trinity College since 1970. He has proved fundamental results in extremal and probabilistic combinatorics, percolation theory and polynomials of graphs, publishing over four hundred papers and ten books.

He has had over fifty Ph.D. students; the UK is today a major power in combinatorics in large part due to him. His pedigree in combinatorics is impeccable: Paul Erdős was his academic father and Bill Tutte his academic uncle. He is a Fellow of the Royal Society, and a Foreign Member of the Hungarian and Polish National Academies of Sciences.

Editor's note: this feature is an extended version of a piece that first appeared in The Fountain.

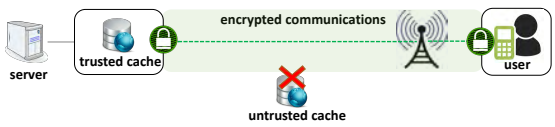
The Future Mathematics of YouTube?

Elizabeth Quaglia

Abstract. We increasingly rely upon video-on-demand services for our entertainment. While we want our video content to be delivered quickly and efficiently, we increasingly want to keep our network demands private. Thus we have two competing needs. In this article we briefly describe how network caching, a key technology enabling efficiency, can be combined with encryption, which provides privacy, highlighting some research directions that could shape the future mathematics of YouTube.

Network efficiency vs. security

Efficiency is one of the fundamental requirements of network communication: when we go online, we would like to access the content we requested as quickly as possible. One way to reduce congestion and improve latency (i.e., the delay before data transfer begins) in communication is to replicate the most popular content in strategic places in the network, i.e., on *caches*. A cache temporarily stores some of a server's content closer to the end user, so that if the same content is requested multiple times the time and bandwidth used to deliver it are greatly reduced. Network caching (i.e., the act performed by the caches) has proved to be a very useful tool in Content Delivery Networks (CDNs), mitigating the burden of the rapidly increasing network traffic often in the form of Video-on-Demand (provided by the likes of YouTube and Netflix). And, considering that CDNs are estimated to deliver over 70% of video traffic by 2019 [1], caching represents an essential technology to ensure the efficiency of future networks.



As our expectations of privacy online mature, another trend is rising in network communication: *end-to-end encryption*. This ensures that a user's request remains *confidential*, i.e., it is only known to the user and the end server from which the content is requested. Web giants such as Facebook, Google, and YouTube are already encrypting their content by default, and it was suggested in [2] that, currently, around 70% of traffic is encrypted.

Until recently, network caching and confidentiality were believed to be conflicting requirements: how can a cache perform its task, namely intercept requests for the same content and deliver it back to the user, if only the user and the end server know what the content is?

CryptoCache: caching with confidentiality

Recently, Leguay et al. [3] disproved that belief by proposing CryptoCache, a security protocol that enables caching of encrypted content that satisfies confidentiality. The main idea behind CryptoCache (see "The CryptoCache protocol" for full details) is for each file to be associated with a pseudo-identifier (pid) and an encryption key (kid), stored by the server. The pseudo-identifier will allow the cache to perform its task, i.e., identify identical requests, without actually knowing what file has been requested, and the key is used to securely transmit the file itself.

Intuitively, CryptoCache satisfies confidentiality since both the file request and the file itself are encrypted with keys only known to the user and the server: the cache (similarly to any other eavesdropper) only sees these values encrypted. This is a great improvement over the state of the art, where, to perform its task, the cache needs to be trusted, i.e., know what file is being requested. However, the protocol, albeit simple, has a drawback: pseudo-identifiers and encrypted files remain constant across requests, and therefore same requests from users can be linked. [3] addresses this by extending CryptoCache to additionally satisfy *unlinkability*, and further analyses key-update strategies to prevent the cache from exhaustively searching the server's database.

The CryptoCache protocol

Let S be the origin server which associates each item of content F with an identifier *id*, a pseudo-identifier *pid*, and a symmetric encryption key *kid*. Let C be a cache, and caches associate pseudo-identifiers with encrypted content, e.g., C might associate *pid* with the encryption of *F* under key *kid*, denoted $\text{Enc}_{kid}(F)$. The protocol consists of three phases: *Setup*, *Request* and *Response*.

- **Setup**. User U and server S share a secret key s, established prior to each run of the protocol.
- **Request**. To request a file F, user U encrypts the file's identifier *id* with s and sends the resulting value, called ciphertext, to server S. This is,

  - $U \longrightarrow S$: $\text{Enc}_s(id)$.
- **Response**. To respond to a request, S decrypts the received ciphertext using s to recover the file identifier, it looks-up the corresponding encryption key *kid*, it encrypts *kid* with s, and sends the resulting ciphertext together with *pid* to the cache C, which is closer to the user. This is denoted by

  - $S \longrightarrow C$: *pid*, $\text{Enc}_s(kid)$.

  If a *cache miss* occurs, i.e., the cache is not storing *pid* and associated encrypted content, then cache C sends *pid* back to the server, which responds with the encryption of the desired file F under encryption key *kid*. Namely,

  - $C \longrightarrow S$: *pid*,
  - $S \longrightarrow C$: $\text{Enc}_{kid}(F)$.

  Now that cache C is storing *pid* and associated encrypted content, it sends the latter along with the encrypted encryption key to user U. We note that, crucially, if a cache hit occurs, i.e., the cache *is* storing *pid* and associated encrypted content, the above step would not be required. We denote this step as

  - $C \longrightarrow U$: $\text{Enc}_s(kid)$, $\text{Enc}_{kid}(F)$.

  Upon receipt, user U can recover the encryption key using s, the secret key it shares with the server, and decrypt the second ciphertext to finally obtain the file it requested.

A new caching trend

Caching involves storing popular files closer to the user so that multiple requests for the same file are responded to more efficiently. Traditionally, the *entire* file is stored on the cache, however, recently, a new caching trend has successfully emerged: *coded caching*. The idea behind coded caching is to pre-fill the caches with *shares* of the popular files in moments of low network traffic (at night, for instance), and to broadcast to the network the missing file shares when files are actually requested.

More precisely, let S denote a server storing a collection of files. Let n be the number of files $F_1, F_2, ..F_n$ stored in S.

A coded caching scheme works in two phases: first there is a *placement phase*, followed by a *delivery phase*. In the placement phase the caches are populated with content related to the n files, without any prior knowledge of future file requests. In the delivery phase, each user requests one of the n files to the server, via the cache, and the server broadcasts to the network a single reply to all the requests. This reply, combined with the content stored on the cache, will allow the user to receive the requested file. The benefit of this approach is that, at peak traffic time, the network will be less burdened, since, ideally, sending the broadcast reply will be "lighter" than transmitting the entire files.

Two examples from [4] of coded caching schemes that achieve optimal transmission rate are given in "Coded caching schemes". While these are simple examples to illustrate the idea of coded caching, the results in [3] and related works (e.g., [5]) provide general coded caching schemes for all parameters as well as lower bounds on the optimal server transmission rate. Crucially, the schemes proposed in the literature ensure that requested files are protected from an eavesdropper (i.e., an eavesdropper cannot learn what file is being requested), but confidentiality is not provided with respect to the cache, which knows exactly what files are being requested.

What next?

There are a number of interesting research directions in this exciting area. First and foremost, Paschos, Quaglia and Smyth are investigating how to extend

Coded caching schemes

Example 1: the server stores two files F_1 and F_2, and there are two caches. Let F_1^1 and F_1^2 be bit-strings partitioning file F_1 into equal shares, and, similarly, F_2^1 and F_2^2 for F_2. Let t_1 and t_2 be two independent and uniformly distributed random keys, each of size $|F|/2$. And let C_1 and C_2 be the two caches. In the placement phase, server S assigns the following data to the caches (note $\oplus$ indicates bitwise XOR):

- in C_1: $F_1^1 \oplus F_2^1 \oplus t_2$, t_1
- in C_2: $F_1^2 \oplus F_2^2 \oplus t_1$, t_2

In the delivery phase, suppose user 1 requests F_1 to cache C_1 and user 2 requests F_2 to C_2. The server broadcasts

$$F_1^2 \oplus t_1, F_2^1 \oplus t_2.$$

It is easy to verify that each user receives the requested file since the cache can recover it from the data it stores and the content S has transmitted in the delivery phase.

Example 2: the server stores three files F_1, F_2, and F_3 and there are three caches, C_1, C_2, and C_3. Similarly to the previous example, the files are partitioned into three equal shares, but in this solution no keys are required. In the placement phase, server S assigns the following data to the caches:

- in C_1: (F_1^2, F_1^3), (F_2^2, F_2^3), (F_3^2, F_3^3)
- in C_2: (F_1^1, F_1^3), (F_2^1, F_2^3), (F_3^1, F_3^3)
- in C_3: (F_1^1, F_1^2), (F_2^1, F_2^2), (F_3^1, F_3^2)

In the delivery phase, suppose user 1 requests F_1 to cache C_1, user 2 requests F_2 to C_2 and user 3 requests F_3 to cache C_3. The server simply broadcasts

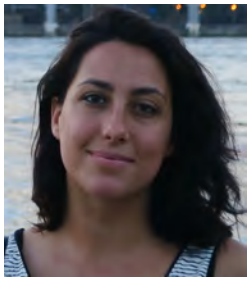
$$F_1^1 \oplus F_2^2 \oplus F_3^3.$$

Since every cache has all the file shares except the ones being broadcast, the correct files can be reconstructed and transmitted to the user.

CryptoCache to the coded caching setting. The main challenge here is to develop technology to identify and reconstruct the correct file in a confidential way, without having to trust the cache. Secondly, recent results in Private Information Retrieval using techniques from distributed storage could be an interesting and promising area to explore in relation to the problem of confidential coded caching. And, finally, in [3] a possible implementation of CryptoCache over HTTP is discussed. It would be extremely interesting and of practical relevance to consider how to incorporate confidential coded caching results in real-world scenarios, so that this research would truly be helping to create the future mathematics of YouTube.

REFERENCES

[1] Cisco, Cisco visual networking index: Global mobile data traffic forecast update 2014-2019, 2015.
[2] Sandvine, Report on global internet phenomena spotlight: Encrypted internet traffic, White paper, 2016.
[3] J. Leguay, G.S. Paschos, E.A. Quaglia and B. Smyth, CryptoCache: Network Caching with Confidentiality, IEEE ICC, 2017.
[4] V. Ravindrakumar, P. Panda, N. Karamchandani and V. Prabhakaran, Fundamental Limits of Coded Caching, IEEE International Symposium on Information Theory, 2016.
[5] A. Sengupta, R. Tandon and T.C. Clancy, Fundamental limits of caching with secure delivery, IEEE Transactions on Information Forensics and Security, 2015.



Elizabeth Quaglia

Elizabeth Quaglia is a Lecturer in the Information Security Department at Royal Holloway, University of London. Her area of expertise is cryptography, with special focus on public-key encryption. She is especially interested in secure anonymous broadcast encryption schemes and cryptographic protocols with functionalities such as e-voting and e-auctions.

A Panoply of Proofs that there are Infinitely Many Primes

ANDREW GRANVILLE

Abstract. There are many different ways to prove that there are infinitely many primes. I will highlight a few of my favourites, selected so as to involve a rich variety of mathematical ideas.

Different types of proofs

Proofs by contradiction

Proofs that there are infinitely many primes typically rely on the theorem that

Every integer $q > 1$ has a prime factor.

Euclid used this to prove that there are infinitely many primes, as follows: Suppose that $p_1, \dots, p_k$ is a complete list of all of the primes. Now $q = p_1 \cdots p_k + 1$ is divisible by some prime p. But then $p = p_j$ for some j and so $q \equiv 1 \pmod p$, so that $(q, p) = 1$, a contradiction. □

There are many variations on this theme. For instance we can take q to be $p_1 \cdots p_k - 1$, or $mp_1 \cdots p_k + 1$ for any integer $m \neq 0$. We could also split the primes into any two subsets: write $\{p_1, \dots, p_k\} = \mathcal{M} \cup \mathcal{N}$, and then let m be the product of the elements of $\mathcal{M}$, and let n be the product of the elements of $\mathcal{N}$. Finally let $q = m + n$ have prime divisor p. Then p must divide one, and only one, of m and n: if p divides, say, m then $(q, p) = (n, p) = 1$, a contradiction. □

We could also take $q = |m - n|$, and as long as this is not 1 then the analogous argument works, though there are a couple of examples known where $m - n = 1$.[1]

We can have more than two summands: If $N = p_1 \cdots p_k$, let $q = \sum_{i=1}^{k} N/p_i$. Now p_j divides N/p_i whenever $i \neq j$, so $(q, p_j) = (N/p_j, p_j) = 1$. A more flexible variant comes by including coefficients $c_1, \dots, c_k$ where each c_j is an integer that is not divisible by p_j, and then $q = \sum_{i=1}^{k} c_i\, N/p_i$. This is so flexible that if $p_1, \dots, p_k$ are the primes up to x, then each prime between x and x^2 equals such a q, for carefully selected values of the c_j (see [1]).

The key idea in Euclid's proof is that q is an integer that is greater than 1 and coprime to $N = p_1 \cdots p_k$. This can easily be generalized as Euler showed that there are $(p_1 - 1)(p_2 - 1) \cdots (p_k - 1)$ positive integers that are at most N and are coprime to N, so we could have taken q to be any such integer greater than 1.

A (point-set) topological proof

One of the most elegant ways to present Euclid's idea is in Furstenberg's extraordinary proof [5] using basic notions of point set topology.

Define a topology on the set of integers $\mathbb{Z}$ in which a set S is open if it is empty or if for every $a \in S$ there is an arithmetic progression

$$\mathbb{Z}(a, m) := \{a + nm : n \in \mathbb{Z}\},$$

with $m \neq 0$, which is a subset of S. Evidently each $\mathbb{Z}(a, m)$ is open, and it is also closed since

$$\mathbb{Z}(a, m) = \mathbb{Z} \setminus \bigcup_{b:\ 0 \le b \le m-1,\ b \neq a} \mathbb{Z}(b, m).$$

If there are only finitely many primes p then $A = \cup_p\, \mathbb{Z}(0, p)$ is also closed, and so $\mathbb{Z} \setminus A = \{-1, 1\}$ is open, but this is false since $\{-1, 1\}$ is finite and so cannot contain any arithmetic progression $\mathbb{Z}(a, m)$, as this would contain infinitely many integers. This contradiction implies that there are infinitely many primes. □

I love the surprising sparse elegance of this proof. However, I know of other number theorists who dislike the way it obscures what is really going on.

An analytic proof

The idea is to count the number of positive integers up to some large point x whose prime factors only come from a given set of primes

[1] Most famously, at least for baseball aficionados, Babe Ruth's home runs record of $714 = 2 \times 3 \times 7 \times 17$ home runs, was overtaken when Hank Aaron hit $715 = 5 \times 11 \times 13$.

$\mathcal{P} = \{p_1 < p_2 < \ldots < p_k\}$. These integers all take the form

$$p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \text{ for non-negative integers } e_j. \quad (1)$$

We are going to count the number of such integers up to $x = 2^m - 1$, for an arbitrary integer $m \geq 1$, by studying this formula. For each j, the prime $p_j \geq 2$, and every other $p_i^{e_i} \geq 1$, and so

$$2^{e_j} \leq p_j^{e_j} \leq p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \leq 2^m - 1.$$

This implies that e_j is at most $m-1$, and so there are at most m possibilities for the integer e_j, the integers from 0 through to $m-1$. Therefore the number of integers of the form (1), up to $2^m - 1$, is at most

$$\prod_{j=1}^{k} \#\{\text{integers } e_j : 0 \leq e_j \leq m-1\} = m^k.$$

Now if $\mathcal{P}$ is the set of all primes then every positive integer is of the form (1), and so the last equation implies that $2^m - 1 \leq m^k$ for all integers m. We select $m = 2^k$, so this implies that $2^k \leq k^2$, which is false for every integer $k \geq 5$. Therefore as we know that there are at least five primes (for example $2, 3, 5, 7, 11$), we can deduce that there cannot be finitely many. □

This proof highlights the use of counting arguments in number theory, a first step on the road to analytic number theory.

Two arithmetic proofs.

Fermat's little theorem implies that if p is an odd prime then

$$2^{p-1} \equiv 1 \pmod{p}.$$

If $2^m \equiv 1 \pmod{p}$ then one can deduce that $2^g \equiv 1 \pmod{p}$ where $g = (m, p-1)$. We will use this observation to give two proofs of the infinitude of primes, both based on arithmetic structure.

• Suppose that there are only finitely many primes and let q be the largest prime. If p is a prime factor of the Mersenne number, $2^q - 1$, then $2^q \equiv 1 \pmod{p}$. Therefore $2^g \equiv 1 \pmod{p}$ where $g = \gcd(q, p-1)$. Now g divides q, so g must equal either 1 or q. However g cannot equal 1, otherwise p divides $2^g - 1 = 1$. Therefore $q = g$ which divides $p-1$. But then $q \leq p - 1 < p$, so p is a larger prime than q, contradicting the maximality of q. □

• Suppose that there are only finitely many primes $p_1, \ldots, p_k$ and let 2^n be the highest power of 2 dividing any $p_j - 1$. Let $q = 2^{2^n} + 1$ be the nth Fermat number. Then $2^{2^{n+1}} - 1 = (2^{2^n})^2 - 1 \equiv (-1)^2 - 1 \equiv 0 \pmod{q}$, and so if p is a prime factor of q then $2^{2^{n+1}} \equiv 1 \pmod{p}$. Therefore $2^g \equiv 1 \pmod{p}$ where $g = \gcd(2^{n+1}, p-1)$. Now g divides 2^{n+1} so g must be a power of 2, say $g = 2^m$. Moreover $m \leq n$ as $g = 2^m$ divides $p-1$, and 2^n was defined to be the highest power of 2 dividing any $p_j - 1$. Therefore

$$0 \equiv q = 2^{2^n} + 1 = (2^{2^m})^{2^{n-m}} + 1$$
$$\equiv 1^{2^{n-m}} + 1 \equiv 2 \pmod{p},$$

so that p divides 2, which is impossible as p is an odd prime. □

This proof also yields that for any integer $N \geq 1$, there are infinitely many primes $\equiv 1 \pmod{2^N}$, and suitable modifications even allow one to prove that for any integer $m \geq 2$, there are infinitely many primes $\equiv 1 \pmod{m}$. In 1837 Dirichlet proved that if $(a, q) = 1$ then there are infinitely many primes $\equiv a \pmod{q}$. Far ahead of his time, Dirichlet used analytic methods to prove this result. There is still no known elementary proof of this fact for all pairwise coprime a and q, though here we have indicated an approach that works whenever $a = 1$.

A proof by irrationality

Euler exhibited the inspiring identity

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \ldots$$

Let $\delta(n) = 1$ or -1 as $n \equiv 1$ or $-1 \pmod{4}$, and $\delta(n) = 0$ if $n \equiv 0 \pmod{2}$. The key observation is that if an odd integer n factors as in (1), then $\delta(n)/n = \prod_{j=1}^{k} (\delta(p_j)/p_j)^{e_j}$. Therefore if there are only finitely many primes then the right-hand side of Euler's identity can be separated into the contributions from each prime to obtain the identity,

$$\frac{\pi}{4} = \left(\prod_{\substack{p \text{ prime} \\ p \equiv 1 \pmod 4}} \frac{p}{p-1} \right) \cdot \left(\prod_{\substack{p \text{ prime} \\ p \equiv 3 \pmod 4}} \frac{p}{p+1} \right).$$

It is well-known that π (and so $\pi/4$) is irrational, but under the assumption that there are only finitely many primes, the right-hand side is a finite product of rational numbers, so is rational, a contradiction. □

The function δ is periodic of period 4; equals 0 whenever $(n,4)>1$, and otherwise equals 1 or -1; sums over its period to 0 (as $1+0+(-1)+0=0$); and factors much like the integers, in that $\delta(n)=\prod_{j=1}^{k}\delta(p_j)^{e_j}$. For every integer $m>2$ with $m\not\equiv 2 \pmod 4$, there exists such a function δ with "4" replaced by "m" in the definition. The sum of Euler's series, $\sum \delta(n)/n$ is the "special value" of Dirichlet's L-function that is central to his proof that there are infinitely many primes in arithmetic progressions. Moreover, much like here, if $m=4k$ where k is not divisible by any squares and $k\equiv 1 \pmod 4$, then the sum adds up to a rational multiple of $\pi\sqrt{|m|}$.

Euler's work pre-dated Dirichlet by almost 100 years, yet he developed the theory of this same mathematical construction without knowing how important it would become. Such prescience can be found in the works of great mathematicians.

A proof by combinatorics and arithmetic geometry

Van der Waerden's Theorem, a deep result in combinatorics, states that for any given $m\ge 2$ and $\ell\ge 3$, if every positive integer is assigned one of m colours, in any way at all, then there is an ℓ-term arithmetic progression of integers which each have the same colour. Alpoge [3], a current Ph.D. student at Harvard, suggested the following clever colouring of the integers, assuming that $p_1,\dots,p_k$ are all the primes. Each integer n factors as in (1); we write each exponent $e_j\equiv r_j \pmod 2$ with $r_j=0$ or 1. Writing $R=p_1^{r_1}\cdots p_k^{r_k}$ we note that n/R is the square of an integer, and we "colour" n with the colour R. There are 2^k possibilities for R. By applying van der Waerden's Theorem with $m=2^k$ and $\ell=4$ we deduce that there are four integers in arithmetic progression

$$A, A+D, A+2D, A+3D, \text{ with } D\ge 1,$$

which all have the same colour R. Now R divides each of these numbers, so also divides $D=(A+D)-A$. Letting $a=A/R$ and $d=D/R$, we deduce that

$$a,\ a+d,\ a+2d,\ a+3d$$

are four squares in arithmetic progression ($a+jd=(A+jD)/R$ is a square as $A+jD$ has colour R.) However Fermat proved (and this is often covered in a first course on elliptic curves) that there cannot be four squares in an arithmetic progression. □

Although this proof uses two far deeper theorems than Euclid's original proof, one cannot help but be charmed by how they can be combined in this way. Actually these ideas have come together before in an unlikely way (see [4]), in bounding the number of squares that can possibly appear in an N-term arithmetic progression.

The construction of infinitely many primes.

We want to construct an infinite sequence of distinct, pairwise coprime, integers $a_0, a_1, \dots$; that is, a sequence for which $\gcd(a_m,a_n)=1$ whenever $m\ne n$. Let p_n be a prime divisor of a_n whenever $|a_n|>1$. Then the p_n form an infinite sequence of distinct primes. (For, if not, then $p_m=p_n$ for some $m\ne n$ and so $p_m=(p_m,p_n)$ divides $(a_m,a_n)=1$, a contradiction.) Here a couple of ways to construct such sequences:

• Modification of Euclid's proof: Let $a_0=2, a_1=3$ and

$$a_n=a_0a_1\cdots a_{n-1}+1 \text{ for each } n\ge 1.$$

If $m<n$ then a_m divides $a_0a_1\dots a_{n-1}=a_n-1$ and so $\gcd(a_m,a_n)$ divides $\gcd(a_n-1,a_n)=1$, which implies that $\gcd(a_m,a_n)=1$. Therefore if p_n is a prime divisor of a_n for each $n\ge 0$, then $p_0,p_1,\dots$ is an infinite sequence of distinct primes.

The recurrence for the a_n can be re-written as

$$\begin{aligned} a_{n+1}&=a_0a_1\cdots a_{n-1}\cdot a_n+1\\ &=(a_n-1)a_n+1=f(a_n),\end{aligned}$$

where $f(x)=x^2-x+1$, which leads us to a different proof that these numbers are pairwise coprime. We use the fact that for any distinct integers r and s, and any polynomial $f(x)\in\mathbb{Z}[x]$, $r-s$ always divides $f(r)-f(s)$. Therefore if $r\equiv s \pmod p$ then $f(r)\equiv f(s) \pmod p$. Therefore if p divides a_n then $a_{n+1}=f(a_n)\equiv f(0)=1 \pmod p$. Next $a_{n+2}=f(a_{n+1})\equiv f(1)=1 \pmod p$, and then $a_{n+3}=f(a_{n+2})\equiv f(1)=1 \pmod p$, and proceeding like this,

$$\begin{aligned} a_{n+k}&=f(f(f(\dots f(a_{n+1})\dots)))\\ &\equiv f(f(f(\dots f(1)\dots)))\equiv 1 \pmod p,\end{aligned}$$

for all $k\ge 1$; and so we deduce that $a_m\equiv 1 \pmod p$ for all $m>n$. We deduce that a_m and a_n cannot share any prime factor p, and so are coprime. □

• Fermat claimed that the integers $F_n=2^{2^n}+1$ are primes for all $n\ge 0$. This is true for

$3, 5, 17, 257, 65537$, but false for $F_5 = 641 \times 6700417$, as noted by Euler.[2] Nonetheless the F_n are pairwise coprime, and so we can deduce that if p_n is a prime divisor of F_n, then $p_0, p_1, \ldots$ is an infinite sequence of distinct primes. To prove this we begin by noting that the F_n-values can be determined by a simple recurrence, as follows:

$$\begin{aligned} F_{n+1} &= (2^{2^n}+1)(2^{2^n}-1)+2 \\ &= F_n(F_n-2)+2 = f(F_n), \end{aligned}$$

where $f(x) = x^2 - 2x + 2$. Hence if $p|F_n$ then $F_{n+1} = f(F_n) \equiv f(0) = 2 \pmod{p}$, and $F_{n+2} = f(F_{n+1}) \equiv f(2) = 2 \pmod{p}$; continuing like this we have

$$\begin{aligned} F_{n+k} &= f(f(f(\ldots f(F_{n+1})\ldots))) \\ &\equiv f(f(f(\ldots f(2)\ldots))) \equiv 2 \pmod{p}, \end{aligned}$$

for all $k \geq 1$, and so we deduce that $F_m \equiv 2 \pmod{p}$ for all $m > n$. But since each prime factor p of F_n is odd (as F_n is odd), we deduce that the F_n are pairwise coprime. □

When you see two proofs like these last two proofs, that are so similar, you begin to suspect that there may be some deeper unifying idea lying not far below the surface. We explore an appropriate generalization in the next section.

The arithmetic of dynamical systems

Orbits, periods and pre-periods

We have shown above that the $(a_n)_{n\geq 0}$ and the $(F_n)_{n\geq 0}$ are both examples of sequences $(x_n)_{n\geq 0}$ for which x_0 is given and then

$$x_{n+1} = f(x_n) \quad \text{for all } n \geq 0,$$

for some polynomial $f(x) \in \mathbb{Z}[x]$; the a_n with the polynomial $x^2 - x + 1$, and the F_n with the polynomial $x^2 - 2x + 2$. Such sequences are examples of *dynamical systems*, in which the next value of a function depends on its current value. The numbers $(x_n)_{n\geq 0}$ are the *orbit* of x_0 under the map $x \to f(x)$. Both proofs used a *period* which means that in, say, the orbit of y_0, we have $y_n = y_0$. This implies that $y_{n+j} = y_j$ for all $j \geq 0$, which follows from induction by noting that $y_{n+j+1} = f(y_{n+j}) = f(y_j) = y_{j+1}$.

In our two examples, the key to proving coprimality is that 0 is *pre-periodic* (i.e. the orbit of 0 eventually becomes periodic but 0 is not in the period): For $f(x) = x^2 - x + 1$ we have

$$\boxed{0 \to 1 \to 1 \to \ldots}$$

and for $f(x) = x^2 - 2x + 2$ we have

$$\boxed{0 \to 2 \to 2 \to \ldots}$$

One can classify the polynomials for which the orbit of 0 is eventually periodic, and so come up with many more proofs that there are infinitely many primes! There is a big surprise; any period in a dynamical system $x \to f(x)$ with $f(x) \in \mathbb{Z}[x]$ has period length 1 or 2. This can be used to prove that if 0 is pre-periodic for the map $x \to f(x) \in \mathbb{Z}[x]$ then the orbit of 0 must be one of the following four basic possibilities (each given here with examples of polynomials for which 0 has that orbit):

• The polynomial $f(x) = x^2 - ax + a$, indeed any polynomial of the form $a + x(x-a)g(x)$ where $g(x) \in \mathbb{Z}[x]$, has the orbit

$$\boxed{0 \to a \to a \to \ldots}$$

• The polynomial $f(x) = x^2 - 2$ gives the case $a = 2$ in the orbit

$$\boxed{0 \to -a \to a \to a \to \ldots}$$

One can find such orbits with $a = -2, -1, 1$ or 2.

• The polynomial $f(x) = x^2 - ax - 1$ gives the case with the minus sign in the orbit

$$\boxed{0 \to \pm 1 \to a \to \pm 1 \to \ldots}$$

• The polynomial $f(x) = 1 + x + x^2 - x^3$ gives the case with the plus sign in the orbit

$$\boxed{0 \to \pm 1 \to \pm 2 \to \mp 1 \to \pm 2 \to \ldots}$$

(In the last two possibilities one can obtain the case with the other sign by replacing $f(x)$ with $-f(-x)$.)

[2] It is an open question as to whether there are infinitely many Fermat primes, F_n. We have listed the only F_n known to be prime, and for $5 \leq n \leq 30$ the F_n are composite, and for many other n besides. It could be that all F_n, $n > 4$ are composite, or they might all be prime from some sufficiently large n onwards. We have no way of knowing what exactly is true.

Proof that all periods have length 1 or 2.

Suppose that N is the smallest positive integer for which $a_N = a_0$, so that $a_{N+j} = a_j$ for all $j \geq 0$ (as noted above).

Assume that $N > 1$ so that $a_1 \neq a_0$. Now $a_{n+1} - a_n$ divides $f(a_{n+1}) - f(a_n) = a_{n+2} - a_{n+1}$ for all $n \geq 0$, and so $a_1 - a_0$ divides $a_2 - a_1$, which divides $a_3 - a_2, \ldots$, which divides $a_N - a_{N-1} = a_0 - a_{N-1}$; and this divides $a_1 - a_N = a_1 - a_0$, the non-zero number we started with. We deduce that $|a_{j+1} - a_j| = |a_1 - a_0|$ for all j. The integers $a_{j+1} - a_j$ cannot all be equal or else

$$0 = a_N - a_0 = \sum_{j=0}^{N-1} (a_{j+1} - a_j)$$
$$= \sum_{j=0}^{N-1} (a_1 - a_0) = N(a_1 - a_0) \neq 0,$$

a contradiction. Therefore there must be some $j \geq 1$ for which $a_{j+1} - a_j = -(a_j - a_{j-1})$, and so $a_{j+1} = a_{j-1}$. Therefore N, the period length, equals 2. □

Final remarks

There are other proofs, many other proofs, that there are infinitely many primes. Some are quite similar to those mentioned here, others are rather different. Some lead to deeper, rich veins of mathematical thought, others are isolated gems, though some are little more than a reformulation of the ideas already known. But it is always a treat to see a new proof and to think through how it fits into the literature and where it leads. Proofs can be found by people at different levels of their education, for example [3] (discussed in section 12) was discovered by a student, and is the most original and interesting new proof in years.

Other sources for different proofs of the infinitude of primes include the very popular [2], my own personal favourite, [6], which is a rich (though slightly out-of-date) resource for many things about primes, and the website http://www.cut-the-knot.org/proofs/primes.shtml.

Once one knows that there are infinitely many primes, one cannot help but wonder how many are there up to a given point? For example, does the count grow as fast as the count of the number of squares? Or, one might want a big prime and so ask how does one go about finding and identifying primes, and how long should one expect to take to do so?

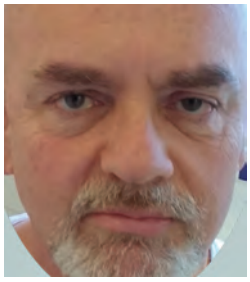
One might ask whether there are infinitely many primes in a given arithmetic progression; and since the arithmetic progression $a \pmod q$ can be viewed as the values of the polynomial $a + nq$ as n runs through the integers, one might ask whether there are infinitely many prime values of, say, the polynomial $n^2 + 1$, or any other irreducible polynomial.

One might ask whether there is a formula for primes and, if so, is it is a useful formula?

We have answers to some of these questions but not all. And even the answers beg further questions, so that the possibilities are limitless, and always so intriguing.

REFERENCES

[1] T. Agoh, P. Erds, and A. Granville, Primes at a (somewhat lengthy) glance. Amer. Math. Monthly 104 (1997), 943–945.
[2] M. Aigner and G. M. Ziegler, Proofs from The Book (5th edn) Springer-Verlag, Berlin, 2014.
[3] L. Alpoge, van der Waerden and the primes. Amer. Math. Monthly 122 (2015), 784–785.
[4] E. Bombieri, A. Granville, and J. Pintz, Squares in arithmetic progressions. Duke Math. J. 66 (1992), 369–385.
[5] H.Furstenberg, On the infinitude of primes. Amer. Math. Monthly 62 (1955), 353.
[6] P. Ribenboim, The new book of prime number records. Springer-Verlag, New York, 1996.
[7] B. Rice, Primitive prime divisors in polynomial arithmetic dynamics. Integers 7 (2007), A26.



Andrew Granville

Andrew Granville specializes in understanding the distribution of primes, and is co-developer of the *pretentious approach* to analytic number theory. He is co-author of the soon-to-appear graphic novel, *MSI; Anatomy and Permutations* (Princeton University Press, 2018). He is chair of pure mathematics at University College London, as well as the Canadian Research Chair in number theory at the Université de Montréal. This article was developed from the author's 2016 London Taught Course Centre Christmas lecture.

Reciprocal Societies: The Italian Mathematical Society

The Unione Matematica Italiana (UMI) was created in response to the International Research Council's plea in July 1919 for the establishment of national scientific committees. At the time, Italy was represented by the Accademia Nazionale dei Lincei and, in particular, by the mathematician Vito Volterra. Voltera, together with a group of mathematicians who included Luigi Bianchi, Pietro Burgatti, Roberto Marcolongo, Carlo Somigliana and Giovanni Vacca, proposed the foundation of the UMI. The first program outline stated some of the aims of the UMI as to encourage pure science, the coming together of pure mathematics and other sciences, the guidance and progress of teaching, and the organization, preparation and participation to national and international conferences.

The Accademia dei Lincei happily welcomed the proposal for the foundation of the UMI and, on 18 March 1921, Volterra informed the famous mathematician from the University of Bologna, Salvatore Pincherle, that he had been chosen as its first President. The official origin of the UMI, however, dates to 31 March 1922 when Pincherle sent a letter presenting the program of the Association to all Italian mathematicians. This letter included the intensions that the UMI be a true professional association with an autonomous structure not unlike the one of other existing international associations.

The society has been very active right from its foundation. By June 1922 the society had 152 members. Since then the membership of the UMI has been gradually increasing, reaching a current membership of about 2000. In July 1922 the first issue of what would become the Bollettino dell'Unione Mathematica Italiana (BUMI) was published, and the Statutes were approved by the UMI on 7 December 1922.

The first act of international importance by the UMI was the organization of the International Congress of Mathematicians held in Bologna in 1928. On that occasion Pincherle, who was also President of the UMI, spent much time and energy (as evidenced by the rich correspondence preserved in the historical archive of the UMI) to reaffirm the international nature of science, inviting for the first time after World War I all countries to participate.

His project, although at first politically opposed by various countries, was successful: the 826 mathematicians from 36 countries, including Germany, participated without any restrictions.

The UMI website is http://umi.dm.unibo.it/. Recently a strong effort has been made to make the website more effective. In it you can find news about UMI, the public positions taken by UMI, various information about the Italian mathematics community, and an updated list of employment opportunities in Italy and abroad. The UMI collaborates with the website Maddmaths! http://maddmaths.simai.eu/ which is devoted to dissemination of mathematics.

As part of the project of reorganisation and valorisation of the UMI Historical archive, an analytical inventory of the document collection and of the papers describing the archival heritage has recently been completed. In the near future it will be possible for the public to consult the archive. The task of rearranging the archive has revealed papers of high interest. These papers attest not only to significant moments and great human and scientific personalities, but also to critical episodes in the history of the UMI. I am referring here specifically to the attitude of UMI management in the period of racial laws and to UMI relationship with Fascism. The reorganization of the archive and the possibility to consult it is in my opinion, beyond rhetorical statements, a late but sincere act of reparation toward those mathematicians who were persecuted by the racial laws of that time.

Ciro Ciliberto
President of U.M.I.

Editor's note: the LMS and the UMI have a reciprocity agreement meaning members of either society may benefit from discounted membership of the other.

Success Stories in Mathematics

What does it mean to be a successful mathematician? What is involved in a successful mathematical career? The LMS Success Stories project aims to celebrate the diversity of successful careers and mathematicians. We are always interested in new profiles! If you have an idea, or would like to submit your own profile, please email Success.Stories@lms.ac.uk.

Name: Julie Rehmeyer
Job: Freelance maths and science writer

Science writing suits me well. It combines a lot of my interests and skills. I've always loved to write, I enjoy learning new things all the time, I love the flexibility and control I have being self-employed, and over time, I feel like I've been able to write things that make a real difference.

For seven years, I wrote the Math Trek column for *Science News*. I loved it, because through the different stories, I could paint a picture of the breadth of mathematics. I was trying to show people all the different things mathematics can be, and to let them see the beautiful and surprising things that are revealed when you look at the world through a mathematical lens.

And people really loved the column – for years, it was the single most popular thing on the entire Science News website. People of course have often had such traumatic experiences with math, but my experience is that means they get even more excited when they read something about math and find that they can understand and enjoy it. It felt to me like a small way of healing some of the wounds of this world.

For many years, I struggled with chronic fatigue syndrome. Freelancing was great because it could accommodate the ups and downs in my health. I've written a book about my experiences with chronic fatigue syndrome, describing the science, politics and history of the disease and other poorly understood illnesses. It's called Through the Shadowlands: A Science Writer's Odyssey into an Illness Science Doesn't Understand. www.throughtheshadowlands.com.

Name: Joanne Dunster
Job: Postdoctoral researcher in mathematical biology, University of Reading

My route into mathematics is unusual. I left school at 16 to take an Engineering Apprenticeship. I then quickly moved into the IT industry, eventually working as an Oracle DBA for a wide range of companies such as Rolls Royce, Powergen & Levi's. While working I took a maths degree with the Open University. I loved this so much that once it was finished I packed up my career in IT and took a PhD in Mathematical Biology.

I now, at a very late stage in life, have my dream job. I work alongside biologists in a Cardiovascular lab developing mathematical models to help to understand the mechanisms that lead to cardiovascular disease.

This section is for Early Career Researchers. Please send suggestions for questions or topics you would like to see covered to newsletter@lms.ac.uk.

Boosting Job Prospects

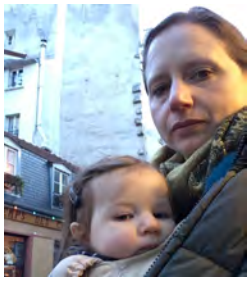
"Dear X, I am a PhD student / postdoc and I'll be moving onto my next position in the next year or so. I'd like a job outside academia. Can you suggest things I can do in the next few months to enhance my CV?"—We invite five professionals to comment.

Ashley Pitcher is an Engagement Manager at QuintilesIMS in London, with a DPhil in mathematical modelling and optimal control of constrained systems from the University of Oxford.

The first thing I would recommend is to decide in which industry you are most interested. Then I would try to gain some basic knowledge of that industry if it is not related to your current research. For example, one of the areas I work in is health economics. We are constantly looking for new hires with great technical skills and understanding of mathematics and statistics. However, it is crucial for applicants to demonstrate some basic knowledge and interest in the area of application. This could be through taking a short course offered through a university or even through a free online course. I would also try to get in touch with any alumni from your university who are already working in that area. A lot of employers have employee referral schemes so applying for a job via an alumnus is the best way to ensure your CV doesn't get overlooked, and they may be able to give you some helpful advice too.

Robert Leese is Chief Technical Officer at the Smith Institute for Industrial Mathematics and System Engineering, and a Fellow of St Catherine's College, Oxford. He has a PhD in mathematical physics from Durham.

Employers like problem-solvers. Mathematicians are often natural problem-solvers, and as a soon-to-be PhD it's a reasonable assumption that you have solved a few problems along the way. However, the problems you've solved have probably been well-posed and you've probably had time to consider everything very carefully and assemble just the right set of tools for the job. The real world is different. Problems arise unexpectedly, and you may have to tackle them without time to do any homework or gather the tools that you would ideally like to use. An employer is unlikely to doubt your ability as a mathematical problem-solver, but more open to question will be your ability to solve problems that crop up "in the wild". Be ready to demonstrate improvisation in problem-solving to a prospective employer. Consider what experience you have in solving problems outside mathematics, especially where there is pressure of time or resources, and where the outcome needs to be "good enough" rather than perfect. Maybe your outside interests will help. Some years ago, I was interviewing a prospective colleague (and still a colleague) at the Smith Institute, who had been involved in the improvised rescue of an injured hiker who had fallen into a cave. "That must have been stressful?", we asked. "Well, nobody died", she replied. The outcome on this occasion was good enough for all concerned!



Ceri Fiddes is Assistant Head at Millfield School, having previously been a Head of Maths for eight years. She got her PhD in Group Theory from Bath University.

Teaching is a great career path to follow if you want to continue to fill your days with conversations about mathematics, the added bonus is that you are regularly provided with captive audiences to talk to. No two classes are ever alike and no two days are the same.

There are a variety of routes into teaching, from a university-based PGCE course to school-centred initial training. Many schools will accept applications from untrained prospective teachers and then undertake to provide training, usually in association with a university or other ITT (Initial Teacher Training) provider. If you are interested in any of these routes you need to make sure that your CV highlights some key skills and experiences. One of the most important things is a passion for mathematics (hopefully not an issue for you) and a genuine desire to inspire this passion in others. You will already be an attractive prospect due to your high level of academic ability, but you will need to convince prospective employers that you also have the necessary (absolutely vital) people skills.

Any experience that you can get working with young people is valuable, not just for your CV but also for the skills that it will develop. Things like working at a summer camp, coaching a team, running masterclasses all look good. The best experience you can get is visiting a school. Most schools will be happy to have a voluntary classroom assistant for a period of time, so get in touch and ask if you can help out. Even better if you can visit a selection of schools and see pupils in a number of settings.

The young people that you inspire will remember you for ever and you may well even shape the rest of their lives. They will be grateful that they happened to end up in your classroom, and you will be grateful that you found a career where you can make such a positive impact.

Adrian Waller is a Thales Expert at Thales UK. He gained a PhD from Royal Holloway, University of London, writing his thesis on graph theory.

As an employer, I would suggest that your knowledge and abilities in mathematics will be taken as given at this stage. In other words, getting that extra paper done or an improved research result will not matter too much. We would be interested in evidence of your understanding of the context in which your work could solve our customers' problems. Importantly, your ability to communicate this to others with a focus on the impact of your work will serve you well. An engineering company like Thales will use some form of demonstration to convince our customers that we understand their problem and can address it. You could consider doing this for your current work or at least a worked example of how it would apply to a real-world use case. This could show potential employers evidence of software, simulation or other relevant skills, but most importantly the ability to put yourself in the mind of those whose problems your work will solve. Believe it or not, many people in industry will not have much mathematical knowledge and in a lot of cases have no interest in the technical details! They will however be very interested if they can understand how it can solve a real world problem, and ultimately add value to their business.

Brian Taylor is a Statistician in a Chemical Development Department at AstraZeneca Pharmaceuticals. He has a BSc in Applied Statistics for Business and Industry from Northumbria University.

The fundamentals you learnt at degree level are your greatest asset. These allow you to apply concepts and learn new techniques relevant to business sectors where you may only have a limited knowledge. Although statistical analysis may interest you in itself, in Pharma, like in many industries, the business is interested in the decisions you make from the analysis, how confident you are in the decision, and the extra business knowledge acquired. The analysis should be as complex as is needed, but no more complex than that. To plan and execute a 'fit for purpose' analysis (i.e., one for making good decisions) you have to be aware of your subject matter. As well as reading about the area, we re-locate and work side by side with subject experts. We work in multidisciplinary teams and no-one is an expert in all areas. A great finding is useless unless you can convey the importance to others so they can apply it. It is important to develop your skills in conveying your expertise and findings so that non-experts understand you. Practise this!

Many businesses now realise the value in applying statistics. However, statistics is still not a normal way of working in the business world so you will need to develop your influencing skills to persuade people to operate in a way unfamiliar to them. You will also need to support them through the process. Your CV should ideally demonstrate examples or at least indicate skills in these capabilities to allow businesses to get the most benefit out of your technical skills.

Micro-theses provide space in the Newsletter for current and recent research students to communicate their research findings with the community. We welcome submissions of micro- and nano-theses from current and recent research students. See http://newsletter.lms.ac.uk for preparation and submission guidance.

Micro-thesis: Free Loop Cohomology of Homogeneous Spaces

Matthew Burfitt

The study of free loop spaces receives great interest from both mathematicians and physicists. Through its study we see a deep unifying nature of mathematics relating geometry, topology and homotopy theory, theory of operads and topological cyclic homology. My PhD project has focused on studying the cohomology of free loop spaces of homogeneous spaces.

Homogeneous spaces

A Lie group is a manifold with a compatible smooth group structure. The simple Lie groups

$$\mathrm{SU}(n),\ \mathrm{Sp}(n),\ \mathrm{Spin}(n),\ \mathrm{G}_2,\ \mathrm{F}_4,\ \mathrm{E}_6,\ \mathrm{E}_7 \text{ and } \mathrm{E}_8$$

can be seen as the building blocks of compact Lie groups and were famously classified by Killing and Cartan in the 1890s with the modern elegant classification by Dynkin diagram due to Dynkin in 1947. Therefore when studying Lie groups or related structures it is most important to first study the simple Lie groups.

In full generality, a homogeneous space is a manifold with a transitive Lie groups action. However, under certain mild conditions, it is also a quotient of a Lie group by a closed subgroup. Examples of homogeneous spaces include Grassmannian manifolds and projective spaces. Also, a complete flag manifold is the quotient of a Lie group by a maximal torus and is one of the nicer examples of a homogeneous space.

Free loop spaces

The free loop space ΛX of a topological space X is an important object of study, particularly when X is a manifold. It is defined to be the topological space of free maps $\mathrm{Map}(S^1, X)$ endowed with the compact open topology.

The motivation for studying free loop spaces mainly comes from their appearance in two areas. Firstly they appear in the theory of geometrically distinct periodic geodesics on a manifold, as originally studied by Gromoll and Meyer in the late 1960s. More recently string topology, the study of algebraic structures on the homology of the free loop space of a manifold, first introduced by Chas and Sullivan in their unpublished 1999 paper, has been an active area of research.

The topology of free loop spaces is well understood for spaces S^n, $\mathbb{C}\mathrm{P}^n$, and for most simple Lie groups. Studying the topology of the free loops space on homogeneous spaces is a natural next step.

Free loop cohomology of complete flag manifolds

The primary tool available for studying free loop spaces from a homotopy theoretic perspective is the free loop fibration

$$\Omega X \to \Lambda X \to X,$$

where ΩX is the topological space of based maps from S^1 to X. In the cases of $X = \mathrm{SU}(n+1)/T^n$ and $\mathrm{Sp}(n)/T^n$ the based loop space can be shown to split, up to homotopy, as a product of $\Omega\mathrm{SU}(n+1)$ or $\Omega\mathrm{Sp}(n)$ and T^n, respectively.

The cohomology of $\mathrm{SU}(n+1)/T^n$ is a quotient of a polynomial algebra by an ideal generated by symmetric functions. To study the cohomology of $\Lambda(\mathrm{SU}(n+1)/T^n)$ we use the cohomology Leray-Serre spectral sequence of the free loop fibration (see “Cohomology Leray-Serre spectral sequences”).

Cohomology Leray-Serre spectral sequences

The cohomology Leray-Serre spectral sequence is a first quadrant spectral sequence arising from a suitable fibration

$$F \to E \to B.$$

This is a sophisticated algebraic tool for studying the cohomology of a spaces using simpler ones. Spectral sequences are usually denoted $\{E_r, d^r\}$, where each page E_r for $r \in \mathbb{Z}_+$, is a differential bigraded algebra $E_r^{p,q}$ with differential of bidegree $(r, 1-r)$. Each subsequent page is obtained from the previous page by computing its homology.
We denote by $E_\infty^{p,q}$ the group $E_r^{p,q}$ such that $E_r^{p,q} = E_{r+k}^{p,q}$ for all $k \geq 0$. The second page of the cohomology Leray-Serre spectral sequence is given by

$$E_2^{p,q} = H^p(B; H^q(F; R))$$

and is a spectral sequence of algebras induced by the algebras $H^*(B; R)$ and $H^*(F; R)$. Provided certain conditions are satisfied the E_∞-page of the spectral sequence will be the associated graded algebra of $H^*(M; R)$.

Despite knowing the cohomology of the base space and the total space of the fibration, no information about the differentials of the associated Leray-Serre spectral sequence can be determined directly. However, there is a map of fibrations from the free loop fibration to the fibration

$$\Omega X \to \mathrm{Map}(I, X) \to X \times X.$$

This fibration is easier to understand as $\mathrm{Map}(I, X) \simeq X$. In the cases of $X = \mathrm{SU}(n+1)/T^n$ or $\mathrm{Sp}(n)/T^n$, I have studied the map of spectral sequences induced by the diagonal map $\Delta\colon X \to X \times X$ and deduced all the differentials in the integral spectral sequence $\{E_r, d^r\}$ associated to the free loop fibration.

Understanding the whole structure of the free loop fibration spectral sequence $\{E_r, d^r\}$ of $\mathrm{SU}(n+1)/T^n$ in one step would be far from straightforward. To reduce complexity, I first considered the differential bigraded algebra (E_2, d^2) before quotienting by the symmetric ideal. This study allowed the complete structure of the E_3-page before the symmetric quotient to be deduced.

In special cases my work resulted in a full description of the structure of the E_3-page of $\{E_r, d^r\}$. This is sufficient to calculate an algebra structure on E_∞ as generators and relations for $H^*(\Lambda(\mathrm{SU}(3)/T^2); \mathbb{Z})$ and $H^*(\Lambda(\mathrm{Sp}(2)/T^2); \mathbb{Z})$. Understanding the topology of objects related to homogeneous space may be useful for applications and my results present a step forward in our understanding of free loop spaces. In addition, the theory behind my computations gives a basis on which to work towards calculations for more complex spaces.

Next Steps

The results of my PhD thesis could be extended more generally to study the free loop cohomology of other homogeneous spaces, in particular to study the cohomology of the complete flag manifolds of other simple Lie groups. To realise this objective I will follow the techniques outlined above. However new methodology would need to be included to tackle more complex multiplicative structures.

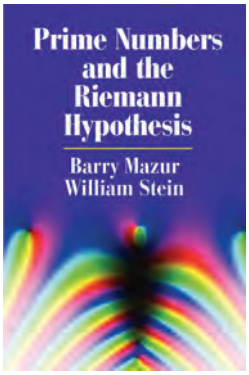
Matthew Burfitt

Matthew Burfitt has just obtained his PhD in mathematics at the University of Southampton under the supervision of Prof. Jelena Grbić. His research interests lie predominantly in homotopy theory and its applications to other areas of mathematics.

Prime Numbers and the Riemann Hypothesis

By Barry Mazur and William Stein, Cambridge University Press, 2016, pp 150, HB £39.99, ISBN 978-1107101920, PB £17.99, ISBN 978-1107499430.

Review by David Singerman



The Riemann hypothesis is possibly the most intriguing unsolved problem in mathematics. Consequently, there has been a large number of popular maths books devoted to it. However, this problem is rather different from other big problems in mathematics, some of which are easily stated and understandable to non-specialists. The usual way to state the Riemann hypothesis is that the non-trivial zeroes of the Riemann zeta function all lie on the line real part of z is equal to ½. This already requires the reader to understand complex functions including analytic continuation, and convergence of infinite series and products. Yet, at heart, this problem is about the distribution of prime numbers and from this viewpoint could possibly be described in a more elementary way.

In a sense, this book is inspired by Zagier's statement quoted in the preface:

> There are two facts about the distribution of prime numbers that I hope to convince you so overwhelmingly that they will be permanently engraved on your hearts. The first is that they are the most arbitrary and ornery objects studied by mathematicians: they grow like weeds among the natural numbers, seeming to obey no other law than that of chance, and nobody can predict where the next one will sprout. The second fact is even more astonishing for it states the opposite: that the prime numbers exhibit stunning regularity, that there are laws governing their behaviour and that they obey these laws with almost military precision.

This short book of 139 pages is divided into four sections. The most elementary part of the book is the first section, just called the Riemann hypothesis. This section comprises 67 pages divided into 24 short chapters. It is mainly concerned with the staircase of the primes, the discrete graph that just plots the nth prime. This is a jagged graph if plotted in the interval $[1, 100]$ but becomes a much smoother curve in the interval $[1, 1000]$ and gets smoother as we increase the second coordinate. This led Gauss at quite a young age to try and find a function which approximated this smooth curve. (A simple way of approximating is that the number of primes up to an integer X is about X divided by twice the number of digits of X.)

Then we are told of Gauss's better approximation $\mathrm{Li}(X)$, where $\mathrm{Li}(X)$ the logarithmic integral of X is defined as the area of the graph of $1/\log t$ for t between 2 and X. Up to this point they are trying to minimize the use of calculus. There are two chapters explaining what is meant by a good approximation and also square root error. They are now ready to give their first formulation of the Riemann hypothesis: "For any real number X the number of prime less than X is approximately $\mathrm{Li}(X)$ and this approximation is square root accurate."

They then form a new staircase by working with the prime powers rather than just the primes and they alter this by having rises at p^n of $\log p$. This gives a new staircase of primes, which essentially gives the Chebychev function $\psi(X)$ and their second formulation of the Riemann hypothesis is "The new staircase is essentially square root close to the 45 degree straight line: i.e. the function $\psi(X)$ is essentially square root close to the function $f(X) = X$."

So far, so good and up to now the book should be accessible to a first year maths student and indeed it would be an excellent supplement to a course on number theory.

The second part is titled *Distributions*. These are generalized functions and this is a topic that few

mathematics undergraduates would tackle. However there are three chapters which give a good idea of the mathematics involved. The first of these is called *How Calculus Manages to Find the Slopes of Graphs that Have No Slopes*. Why are they doing this? It is because the staircase of primes fall into this category.

The third part is called *The Riemann spectrum of the prime numbers*.

Basically they are applying Fourier transforms to the prime staircase graphs. They get periodic graphs with lots of peaks. These peaks are called *The Riemann spectrum*. Then they write, "Riemann defined this sequence of numbers in his 1859 article in a manner somewhat different from the treatment we have given here. In this article they appear as "imaginary parts of the zeroes of the zeta function".

I find this truly amazing! We are nearing the end of the book and this is the first time the zeta function has appeared. The fourth part is called *Back to Riemann* and is relatively straightforward. It ends with the fourth formulation of the Riemann hypothesis—the one that everyone knows. The nontrivial zeroes of the zeta function lie in the complex plane consisting of complex numbers with real part equal to ½.

This is a really interesting book. The first half is elementary but the second half is much more challenging and I learnt a lot of maths reading it. Its hardback version is beautifully produced with lots of colour plates of interesting diagrams (though I have read complaints about the Kindle version). Highly recommended!

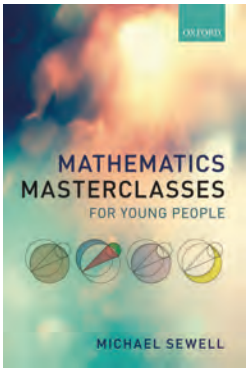
David Singerman

David Singerman is an emeritus professor at the University of Southampton. His main interests have been on Fuchsian groups and Riemann surfaces, in particular the theory of maps (or *dessin d'enfants*) on Riemann surfaces. He has recently retired as the book reviews editor for the *LMS Newsletter*.

Mathematics Masterclasses for Young People

By Michael Sewell, Oxford University Press, 2017, paperback, pp 110, £14.99, ISBN 978-0-19-880121-4.

Review by Charles W Evans



The book begins with an enthusiastic foreword by the late Professor Sir Christopher Zeeman, so we are off to a running start and discover we have a collection of short articles which the author describes as Masterclasses. They originated over a ten year period from classroom work he did once a week with a select group of 10 year old students. Quite a large number of photographs and diagrams are provided and the author says that the book is original in the sense that he has not borrowed material from well-known sources but has developed it himself. Anyone who was at a good school studying mathematics before about 1965 will find a lot of nostalgia in this book. Michael Sewell hopes that it will find favour with young people but many of the younger ones may find it quite difficult at times; for example by page 20 he has launched into algebra with subscripts. The mathematics involved is very traditional; there is not a Venn diagram, a pie chart or a matrix in sight. There is quite a bit of number theory, and geometry plays a significant role. Possibly the book is a little light on content but there are some very good things to be found. He looks for real life opportunities where mathematical ideas can be applied, but in reality the main thing that cements the book together is the extraordinary personality of Michael Sewell himself.

Although I find him entertaining, I can imagine that others might be less enthusiastic. However one can always gain a breather by closing the book and coming back to it a little bit later. His enthusiasm bubbles through and he is probably one of his own greatest fans. There is nothing wrong with this but it does lead to some entertaining situations. For instance in section 79, Lunes, he announces that the problem he is about to discuss has two parts to it but that the time elapsed between the solution of them is about 2420 years. I was intrigued. The first part was proved by Hippocrates of Chios in 410 BC and the second some time in 2013 AD at 3.10am one night by the author himself. The problem is of some interest but it is unlikely that many people struggled during the intervening years to discover and prove it. In section 73, we encounter another feature of interest; Sewell Spirals. He admits this might sound presumptuous but excuses it because the alliteration makes memorising it easier.

There are a few idiosyncrasies; he uses 'guess' rather than 'conjecture'. These words are not synonymous. The latter is usually the result of thought whereas the former could be decided on a whim. He quite rightly emphasises the importance of 'proof' but does not give equal attention to 'definition'. For example in section 17 he defines 'angle' as 'the space between two directions out from a point'. This is meaningless to me but surely all children understand what it means to rotate through a complete revolution and this concept can easily be adapted to give a better notion of angle. The medicine problem (section 14) may satisfy the mathematician in him but I doubt his GP is likely to approve. There are about a dozen ideas that are pseudo-mathematical and really should not be here, for example palindromes and a table of the digits in three languages (85) giving rise to equations such as dix$-$(acht $\times$ due) $= -6$ which is somewhat pointless and does not even have the redeeming feature of being amusing.

On the other hand there is a great deal to commend this book. I may have been aware at one time that the family tree for bees involved the Fibonnacci numbers but if so I had forgotten it and the book has very good illustrations. These could be slightly improved if they were referenced precisely throughout the text because sometimes it is difficult to locate them. He is strong on number theory and geometry. It is almost 60 years since I last considered the 9 point circle and he presents the cardiod nicely. My form master used to introduce it by saying "Now here is a familiar curve". Sewell notes that the word cardiod derives

from heart shaped (but it is not really) but then admits that many young people have no inhibitions in calling it 'bum-shaped', (which it certainly is).

He has a knack of engaging the reader. In 'Supermarket offers: Deal or No Deal' (section 34) I really felt as if I was standing beside him in the store. His premise, which would undoubtedly dismay marketing experts, is that 50% off is not a good deal because the consumer has no way of assessing it. He does not consider taking any account of prices charged by a rival retailer. He is however considerably exercised by the "buy two and get a discount" offers and heads into the supermarket with pen and paper to start recording the prices. Clearly the shop assistant becomes alarmed, possibly suspecting he is some kind of food inspector, and rushes up "Can I help you Sir?", "Not just now, thank you" is the curt reply.

He deliberately doesn't set any homework problems. This is a pity because problems do make the reader less passive and can increase confidence, There are points where it would be a good idea to get the reader actively involved. He does do this occasionally but in the Tethered Goat Problem (section 70) he shows first that 5 tethers suffice and then that 4 will do but does not suggest pupils try to see whether or not 3 will do and if not, why not.

The last three pages are devoted entirely to the author, We get to know quite a lot about him and even see a 3D model of his distinguished head printed on a computer. This book could be an inspiration to young people if the right person is available to guide them.

Charles W Evans

Charles W. Evans spent the better part of his career at Portsmouth where he became Head of Mathematics and Statistics. His research interests are in algebraic graph theory. He is a long standing member of both the LMS and the IMA, where he is an Honorary Secretary. He served on the Science Council Registration Authority for the maximum period and was a Justice of the Peace until the statutory age of retirement. He has been married to Jean for 44 years and they enjoy cruising and have travelled extensively. He is a life member of Hampshire cricket and has four children and seven grandchildren to keep him on his toes.

The Symmetries of Things

By J. H. Conway, H. Burgiel, C. Goodman-Strauss, A K Peters Ltd, 2008, hardback, pp 417, £62.99, ISBN 978-1568812205.

Review by Dave Sixsmith

While there is much that is excellent, including some superb illustrations, this is a deeply frustrating book. But there are also many flaws, some fundamental. This makes a balanced review somewhat problematic. If you want an insight on what is wrong, listen to the authors themselves who – in the introduction – write that "*much of the book was written in hectic three-day sessions .... we usually managed to write several chapters in each session, including one which only arose just then.*" The book is pretty much what one might expect from such an *ad hoc* approach.

It should be said that the book neither attempts nor claims to be a "traditional" text-book. Results are used before being proved, proofs are generally sketched rather than rigorous, and attribution of results is far from complete. The goal seems to be to give the reader sufficient detail and intuition that they can understand the ideas to a certain degree of depth, without drowning them in detail. So long as one takes this as a given, this seems an entirely reasonable, if unusual, approach. In fact it is at times very helpful and refreshing; my clearest understand-

ing of an orbifold comes from the splendid set of pictures in chapter 9.

The book has been divided into three. Part I covers symmetries of finite objects, and repeating patterns in the plane. This is, without doubt, the best part of the book. It starts with four fundamental features of symmetries of a pattern, and introduces a (rather elegant) *signature* to describe how they appear. This leads to the notion of the *cost* of any pattern symbol, and (assuming, for now, a certain upper bound on the cost), the 17 plane pattern symmetries can then be enumerated (and illustrated beautifully). Symmetries on the sphere, and symmetries of friezes are similarly enumerated and illustrated. It is then shown how these "costs" – and the related upper bounds – can be readily deduced from the relevant Euler's characteristic. This is all very intuitive, and elegantly done. This part closes with a review of the classification of closed surfaces, and some pictures of orbifolds.

The choice of terminology is poor; translations are called "wonders" and glide-reflections are called "miracles". This seems just to sow confusion. Apart from this, the first part is excellent. It would be an interesting challenge to build an undergraduate mathematics module using this material. The intuitive and visual nature of the presentation may allow some who generally struggle with pure mathematics to get a deeper understanding than usual.

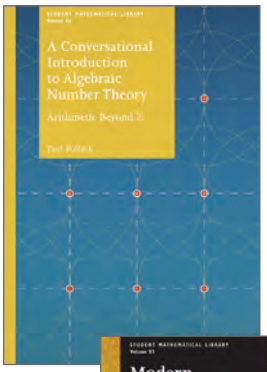
After the first part, things – for this reviewer – proceed downhill rather rapidly. Part II introduces colour symmetries, and increases the level of group theory. The illustrations are the best part. Part III takes discussions of symmetry into other spaces; for example, where in Part I we learn the 17 symmetries for plane patterns, Part III offers the 219 symmetries for space patterns. It is a little overwhelming. The problem is this: the authors tell us that readers of Part II "*are expected to know some group theory*", but Part III "*will be completely understood only by a few professional mathematicians.*" I confess that I firmly lie in the complement of this latter class; Part II was a struggle, Part III completely opaque. It seems that the authors completely lost track of their target audience; I suspect that the "few professional mathematicians" who cope with Part III might find Part I rather woolly.

Grünbaum, in his much longer review of this book for the Amer. Math. Monthly, closes by stating that "*most of us will profit from reading this book, or at least parts of it ....*" This seems, to me, an excellent summary.

Dave Sixsmith

Dave Sixsmith is a research associate at the University of Liverpool. His main research interests are in complex dynamics, complex analysis, and quasiregular dynamics. He came to maths late in life, after careers in programming, IT management, and school teaching. He enjoys hill-walking, cycling and humour. And cake.

AMS
American Mathematical Society



A CONVERSATIONAL INTRODUCTION TO ALGEBRAIC NUMBER THEORY

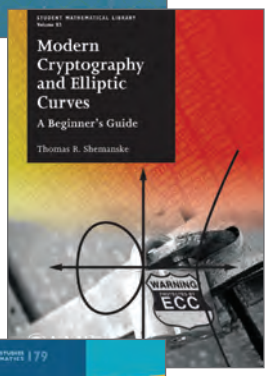
Arithmetic Beyond $\mathbb{Z}$

Paul Pollack, University of Georgia

An introduction to algebraic number theory, meaning the study of arithmetic in finite extensions of the rational number field . Originating in the work of Gauss, the foundations of modern algebraic number theory are due to Dirichlet, Dedekind, Kronecker, Kummer, and others. This book lays out basic results, including the three "fundamental theorems": unique factorization of ideals, finiteness of the class number, and Dirichlet's units theorem.

Student Mathematical Library, Vol. 84

Sep 2017 308pp 9781470436537 Paperback £49.95



MODERN CRYPTOGRAPHY AND ELLIPTIC CURVES

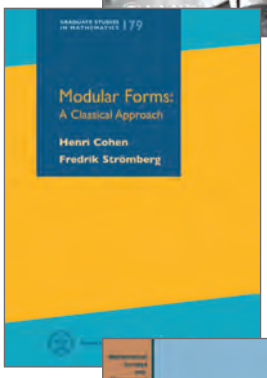
A Beginner's Guide

Thomas R. Shemanske, Dartmouth College

Offers the beginning undergraduate student some of the vista of modern mathematics by developing and presenting the tools needed for an understanding of the arithmetic of elliptic curves over finite fields and their applications to modern cryptography. This gradual introduction also makes a significant effort to teach students how to produce or discover a proof by presenting mathematics as an exploration.

Student Mathematical Library, Vol. 83

Sep 2017 261pp 9781470435820 Paperback £49.95



MODULAR FORMS

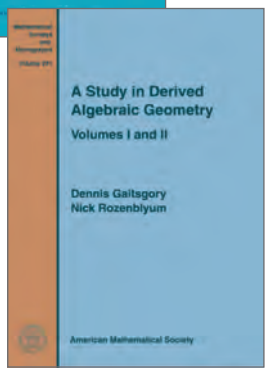
A Classical Approach

Henri Cohen, Université de Bordeaux & Fredrik Strömberg, University of Nottingham

This comprehensive textbook, which includes numerous exercises, gives a complete picture of the classical aspects of the subject, with an emphasis on explicit formulas. The heart of the book is the classical theory developed by Hecke and continued up to the Atkin-Lehner-Li theory of newforms and including the theory of Eisenstein series, Rankin-Selberg theory, and a more general theory of theta series.

Graduate Studies in Mathematics, Vol. 179

Aug 2017 699pp 9780821849477 Hardback £87.95



A STUDY IN DERIVED ALGEBRAIC GEOMETRY

Dennis Gaitsgory, Harvard University & Nick Rozenblyum, University of Chicago

Derived algebraic geometry is a far-reaching generalization of algebraic geometry. It has found numerous applications in various parts of mathematics, most prominently in representation theory. This two-volume monograph develops generalization of various topics in algebraic geometry in the context of derived algebraic geometry.

Volume I: Correspondences and Duality

Mathematical Surveys and Monographs, Vol. 221.1

Sep 2017 553pp 9781470435691 Hardback £125.00

Volume II: Deformations, Lie Theory and Formal Geometry

Mathematical Surveys and Monographs, Vol. 221.2

Sep 2017 463pp 9781470435707 Hardback £125.00

Volumes I and II

Mathematical Surveys and Monographs, Vol. 221

Sep 2017 1016pp 9781470435684 Hardback £220.00

Free delivery at **eurospanbookstore.com/ams**

AMS is distributed by **Eurospan** | group

CUSTOMER SERVICES:
Tel: +44 (0)1767 604972
Fax: +44 (0)1767 601640
Email: eurospan@turpin-distribution.com

FURTHER INFORMATION:
Tel: +44 (0)20 7240 0856
Fax: +44 (0)20 7379 0609
Email: info@eurospangroup.com

Obituaries

Geoffrey Mallin Clarke: 1928 – 2017

Geoffrey Mallin Clarke, who was elected a member of the London Mathematical Society on 17 January 1974, died on 8 May 2017, aged 88.

Charles Goldie writes: After graduating in mathematics at Oxford he stayed on for a Diploma in Statistics, then began his career as the first resident statistician at the Long Ashton Agricultural and Horticultural Research Station. He moved to a lectureship in the Mathematics Division at the University of Sussex in 1966 and was promoted to Reader in 1973. In 1983 he took early retirement and moved to a consultancy role at the University of Kent. It was there that his career blossomed.

He played a key role in the successful merger of the Institute of Statisticians with the Royal Statistical Society, holding office first in the IoS and then in the merged RSS. The project dearest to his heart was statistics education in Africa, where he was involved in university, government and UN programmes in four countries. For his work in retirement he was awarded the Chambers Medal of the RSS in 2001.

An applied statistician now would be unlikely to join the LMS, but Geoff came from an era when it was customary for a rising academic to join and support the learned societies relevant to his field.

Landon Clay: 1926 – 2017

The founder of the Clay Mathematics Institute (CMI) Landon T. Clay passed away on July 29. Clay was a generous benefactor to mathematics and founded CMI in 1998 with his wife, Lavinia D. Clay The primary objective of CMI is to 'encourage the increase and dissemination of mathematical knowledge'.

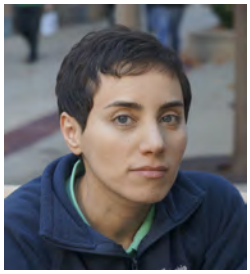
Clay was not himself a mathematician, having graduated from Harvard with a degree in English. His career as a successful businessman and in finance and science-based venture capital funding allowed him to devote his time and energy to philanthropic causes.

CMI is probably best known for the seven Millennium Prize Problems but this is only one of CMI's activities. Other notable activities are the Clay Research Fellowships and the Clay Research Conference and Workshops, where the Clay Research Awards are presented.

Since 2014 the LMS has, in partnership with the CMI, supported 14 Research Schools in the UK, which provided training for young researchers, both students and postdoctoral researchers, in core areas of mathematics. Participants of the Research Schools, both national and international, meet with a number of leading experts from across the world as well as other young researchers working in related areas. The current President of CMI, Professor Nick Woodhouse, was instrumental in setting up this partnership.

More information is available at tinyurl.com/ycrj2tlh

Maryam Mirzakhani: 1977 – 2017



It was with great sadness that the London Mathematical Society learned of the death of Fields Medal winner Maryam Mirzakhani on 15 July 2017 at the age of 40. Mirzakhani became the first woman to receive a Fields Medal in its nearly 80 year history in 2014. She received the award for her 'outstanding contributions to the dynamics and geometry of Riemann surfaces and their moduli spaces'. In essence for her contributions to the fields of topology, geometry, and dynamical systems.

Mirzakhani was born in Tehran in 1977 and obtained her BSc in Mathematics (1999) from the Sharif University of Technology. She then moved to the US to begin her doctorate work at Harvard University, where she received her PhD in 2004. From 2004 to 2008 she was a Clay Mathematics Institute Research Fellow and an assistant professor at Princeton University. She had been a professor of mathematics at Stanford since 2008. While she dreamed of being a writer as a young girl, she chose to follow through her passion for solving mathematical problems.

Maryam was awarded Honorary Membership of the LMS in 2015 and also served on the Editorial Board of the *Journal of Topology* published by the LMS. The Society would like to pass on its sincere condolences to her family and friends.

David Wallace: 1934 – 2017

David Wallace, who was elected a member of the London Mathematical Society on 20 March 1958, died on 31 May 2017, aged 83.

Adam McBride writes: David was born in Cupar, Fife but the family soon moved to Stranraer. Having been dux at Stranraer Academy, he went to St Andrews University where he gained a First Class Honours BSc and was awarded the Miller Prize. At the Victoria University of Manchester he was awarded a PhD for a thesis entitled *On the radical of a group algebra*.

David won a Fulbright Scholarship in 1958 and spent a year as an Instructor at each of Princeton and Harvard. He returned to Scotland in 1960 to start a close association with four more Scottish universities. From a Lectureship at the University of Glasgow, he moved to a Senior Lectureship at the University of Aberdeen in 1965. In 1973 he became a Professor in the University of Stirling, with two stints as Head of Department. His final move was to the University of Strathclyde in 1986. He became Head of Department in 1987 when the department was going through a difficult period. Showing a shrewd mixture of tact and determination, he steered the ship into calmer waters. He was Head of Department for seven years, longer than normal, but this ensured continuity and laid the foundations for a renaissance in the 90s. In addition to departmental responsibilities, David served on a range of high level committees, many of which he chaired.

David was active in several external organisations. He was a long-standing member of the LMS. He served as President of the Edinburgh Mathematical Society and Chair of the Scottish Mathematical Council. He was involved in the early days of the European Mathematical Society. He was elected a Fellow of The Royal Society of Edinburgh in 1978.

David was a perfectionist with a remarkable attention to detail. He had a dry sense of humour but you could usually spot a twinkle in his eye. He was a voracious reader and owned literally thousands of books on a very wide range of subjects. Apart from Mathematics, tennis was a great interest.

Mathematics, particularly in Scotland, has lost a great servant and a prominent member of its community.

Events

Ergodic Theory & Symbolic Dynamics (with a view towards Number Theory)

Location: Queen Mary, University of London
Date: 13–15 September 2017
Website: tinyurl.com/y92orp62

The three-day workshop intends to bring together researchers working in ergodic theory, symbolic dynamics, number theory and combinatorics with the aim of broadening interactions between these subjects. Speakers to include: Simon Baker (Warwick), Karma Dajani (Utrecht), Toby Hall (Liverpool), Thomas Jordan (Bristol), Zuzana Masáková (Prague), Wolfgang Steiner (Paris 7), Polina Vytnova (Warwick), Luca Zamboni (Lyon 1).

The meeting is supported by an LMS Conference grant.

Functor Categories for Groups

Location: Lancaster University
Date: 15 September 2017
Website: tinyurl.com/y7wcpmn6

(Pro-)fusion systems is the second meeting of the Research Group Functor Categories for Groups (FCG). The focus of the meeting will be on the use of fusion systems in the local to global theory of finite groups, and in the theory of profinite groups. Speakers are Markus Linckelmann (City), Ellen Henke (Aberdeen) and Geoffrey Robinson (Lancaster/Aberdeen).

FCG Research Group is supported by an LMS Joint Research Groups in the UK Scheme 3 grant. Limited funding is available for PhD students. To register for the event, email the local organiser Dr Nadia Mazza (n.mazza@lancaster.ac.uk).

LMS Popular Lectures

Location: University of Birmingham
Date: 20 September 2017
Website: tinyurl.com/hu58wjk

The 2017 LMS Popular Lecturers are David Tong (Cambridge) and Jason Lotay (UCL). David Tong will talk on *The Unreasonable Effectiveness of Physics in Mathematics* and Jason Lotay on *Adventures in the 7th Dimension*. The event starts at 6:30pm; refreshments will be at 7:30pm, and the event will end at 9:00pm. Attendance is free. Tickets are available at http://tinyurl.com/y9tvvxvs.

Heilbronn Annual Conference 2017

Location: University of Bristol
Date: 14–15 September 2017
Website: tinyurl.com/y89k48kq

The 2017 Heilbronn Annual Conference will be held in the Chemistry Building at the University of Bristol. A number of distinguished mathematicians are invited to present lectures, intended to be accessible to a mixed audience of mathematicians. There is no registration fee, but to help us plan space and catering, please complete the registration form at heilbronn.ac.uk/events. Support for travel for UK based PhD students may be available. Please contact: heilbronn-coordinator@bristol.ac.uk with any requests by: Thursday 31 August 2017. We welcome applications for caring costs.

LMS Midlands Regional Meeting and Workshop

Location: Loughborough University
Date: 18 September 2017
Website: tinyurl.com/y6vcez4a

Speakers will be Giovanni Felder (ETH, Zurich), Nigel Hitchin (Oxford) and Nikita Nekrasov (Simons Center, Stony Brook). The meeting will be followed by a 3-day workshop on Modern Geometry and Physics, September 19 – 21 (see details of speakers on the website). Funds may be available to support the attendance of UK research students. Enquiries should be addressed to the organisers, H. Ahmadinezhad (h.ahmadinezhad@lboro.ac.uk) and A. P. Veselov (a.p.veselov@lboro.ac.uk).

Operator Theory Workshop

Location: University of Reading
Date: 2–4 October 2017
Website: tinyurl.com/y8s8h6vt

The topics include concrete operators (such as Toeplitz, Hankel and related operators) and their spectra, function spaces (such as Hardy, Bergman and Fock spaces), Riemann-Hilbert problems, and applications in mathematical physics, random matrix theory, and analytic number theory. The workshop is supported by an EPSRC grant and the University of Reading.

LMS–IMA Joint Meeting: Symmetry and Computation

Location: De Morgan House, London
Date: 12 October 2017
Website: tinyurl.com/y72ua87v

The meeting will take place from 11am to 5pm on 12 October. Speakers will be Evelyne Hubert (INRIA Méditerranée), Kurusch Ebrahimi-Fard (Trondheim), Peter Neumann (Oxford), Gloria Marí Beffa (U Wisconsin-Madison) and Darryl Holm (Imperial). The meeting is free to attend. Please register at http://tinyurl.com/y72ua87v.

Categorical Methods in Mirror Symmetry

Location: The University of Kent
Date: 1–2 November 2017
Website: tinyurl.com/yam6sq4v

The meeting will bring together researchers in algebraic geometry, symplectic geometry and mirror symmetry. The speakers contain leading experts and young researchers. One of the intended purposes of the meeting is to put the University of Kent on the map as a centre for research in mirror symmetry, which is the area of specialization of the new lecturers Clelia Pech and Nicolò Sibilla. Funds might be available for UK research students.

The meeting is supported by an LMS Celebrating New Appointments Scheme 1 grant.

BCS–FACS Evening Seminar

Location: De Morgan House, London
Date: 2 November 2017
Website: tinyurl.com/yaprtvdo

This joint event run by BCS–FACS and the London Mathematical Society will be held in the evening of Thursday 2 November. The speaker will be Professor Erika Abraham (RWTH Aachen University), who will talk on *Symbolic Computation Techniques in SMT Solving*. The seminar is free to attend; to register your interest, please email lmscomputerscience@lms.ac.uk.

Discrete Models and KPZ Universality

Location: Durham University
Date: 18 October 2017
Website: tinyurl.com/y947fzzo

An afternoon workshop focusing on probabilistic models such as random tiling models, last passage percolation, directed polymers, etc, and their connection to the KPZ universality class. Talks will be given by Neil O'Connell (Bristol), Kurt Johansson (KTH Stockholm) and Sunil Chhita (Durham).

This meeting is supported by an LMS Celebrating New Appointments Scheme 1 grant.

What is Mathematics Education, Really?

Location: University of Lincoln
Date: 2 November 2017
Website: tinyurl.com/y96le95v

The Annual Boole Lecture in Mathematics will be given by Alexandre Borovik on *What is Mathematics Education, Really?* The lecture will propose that the current crisis in the school level mathematics education means there is increasing pressure to split itin two streams: education for a selected minority who, in their adult lives, will be filling increasingly small share of jobs which really require mathematical competence; and basic numeracy and mathematics awareness classes for the rest of population. After the lecture the audience will be invited to an open discussion of the difficult problem.

Combinatorics and Computation in Groups

Location: ICMS, Edinburgh
Date: 3 November 2017
Website: tinyurl.com/ya4p5dcq

An afternoon meeting around the topic of combinatorics and computation in infinite groups, with talks given by Sarah Rees (Newcastle), Derek Holt (Warwick) and Laura Ciobanu (Heriot-Watt). All are welcome, and some support for young participants is available.

This meeting is supported by an LMS Celebrating New Appointments Scheme 1 grant.

LMS Meeting

Graduate Student Meeting

10 November 2017, 10am–3pm. BMA House, Tavistock Square, London WC1H 7JP

Website: lms.ac.uk/events/society-meetings

These lectures are aimed at a general mathematical audience. All interested, whether LMS members or not, are most welcome to attend this event.

The meeting will include student presentations of their current work, with a prize awarded for the best student talk.

The meeting will be followed by the LMS Annual General Meeting and a reception, which will be held at De Morgan House, 57-58 Russell Square, London, WC1B 4HS.

Travel grants of up to £50 are available for students who attend both the Graduate Student Meeting and the LMS Annual General Meeting.

For further details about the GSM, please contact Anthony Byrne (lmsmeetings@lms.ac.uk)

LMS Annual Dinner
The Society's Annual Dinner will also be held on 10 November at 7.30 pm at the Montague on the Gardens, 15 Montague St, Bloomsbury, London WC1B 5BJ.

The cost of the dinner will be £58, including drinks. To reserve a place at the dinner, please email John Johnston (john.johnston@lms.ac.uk).

LMS Meeting

Annual General Meeting of the LMS

10 November 2017, 3–6pm. BMA House, Tavistock Square, London WC1H 7JP

Website: lms.ac.uk/events/society-meetings

The meeting will open with a brief introduction and a presentation on Society Business. This will be followed by a lecture by **Zoubin Ghahramani** from Cambridge University (*title TBC*), and a presidential address by LMS President **Simon Tavaré**.

These lectures are aimed at a general mathematical audience. All interested, whether LMS members or not, are most welcome to attend this event.

The meeting will include the presentation of certificates to all 2017 LMS prizewinners and the announcement of the Annual LMS Election results.

The meeting will be followed by a reception, which will be held at De Morgan House, 57-58 Russell Square, London, WC1B 4HS.

For further details about the AGM, please contact Elizabeth Fisher (lmsmeetings@lms.ac.uk)

LMS Annual Dinner
The Society's Annual Dinner will also be held on 10 November at 7.30 pm at the Montague on the Gardens, 15 Montague St, Bloomsbury, London WC1B 5BJ.

The cost of the dinner will be £58, including drinks. To reserve a place at the dinner, please email John Johnston (john.johnston@lms.ac.uk).

MathsJam Annual Gathering

Location: Yarnfield Park, Staffordshire
Date: 11–12 November 2017
Website: tinyurl.com/y7wbj8a8

MathsJams are gatherings for like-minded mathematically inclined people interested in problem solving and puzzles. The weekend event consists of lightning talks, long breaks, and plenty of chances to socialise. Come and share, discuss, solve, or be confounded by a vast array of mathematical puzzles in a friendly, informal, and inspirational atmosphere. We're looking for things that are surprising, unexpected, elegant, neat, cool, or whatever just intrigues you.

Flows, Mappings and Shapes

Location: Isaac Newton Institute, Cambridge
Date: 11–15 December 2017
Website: tinyurl.com/ybahqg3c

Computer vision and computer graphics have seen significant recent advances in the analysis of 3D shape through the tools of optimization and flows in shape space. Similarly, long standing problems such as image registration and optical flow are increasingly influencing and benefitting from the computational implementations and representations of diffeomorphic and other mappings. Nevertheless, there is a clear opportunity to further expand and intermix the influence of these methods throughout computer vision. Deadline for applications: 30 September 2017.

Variational Approaches to Problems in Solid Mechanics

Location: University of Warwick
Date: 18 December 2017
Website: tinyurl.com/y9tt8u7f

Solid Mechanics and the Calculus of Variations have been intertwined branches of study since the time of Euler. This workshop will bring together junior faculty members from across the UK who use the techniques of the Calculus of Variations to study models of solid materials. The workshop is supported by an LMS Conference grant and a Leverhulme Early Career Fellowship entitled "A mathematical study of Discrete Dislocation Dynamics".

New Advances in Fano Manifolds

Location: DPMMS, University of Cambridge
Date: 4–8 December 2017
Website: tinyurl.com/yaw4x8ds

This Postgraduate School will introduce PhD students to some recent progress in the geometry of Fano varieties. Fano varieties are of great interest in numerous parts of mathematics such as algebraic, differential and arithmetic geometry. The school will focus in particular on the recent proof of the Borisov-Alexeev-Borisov Conjecture and the classification of Fano foliations with two mini-courses: by Carolina Araujo (IMPA) on *Foliations on Fano varieties*, and Caucher Birkar (Cambridge) on *Linear systems on Fano varieties*.

The school is supported by an LMS Scheme 8 Postgraduate Research Conference grant.

A Random Event in Honour of Ilya Goldsheid's 70th Birthday

Location: Queen Mary, University of London
Date: 18–22 December 2017
Website: tinyurl.com/y8gem8ut

The conference *Classical and Quantum Motion in Disordered Environment* is devoted to three subjects on the interface between mathematical physics, probability and analysis: products of random matrices, the spectral properties of random operators, and random walk in random environment. Particular emphasis will be made on the recent developments in these fields, and on the interrelations between them. The conference is organized in partnership with the CMI, and supported by an LMS Conference grant, the EPSRC, ERC, IAMP, and QMUL.

Theoretical and Algorithmic Underpinning of Big Data

Location: Isaac Newton Institute, Cambridge
Date: 15–19 January 2017
Website: tinyurl.com/yddoedlt

This opening workshop will serve two purposes: first, participants will describe key recent advances in methodology and algorithms for handling large, complex data structures, along with their theoretical underpinnings. Second, we will encourage participants to use this opportunity to map out what they see as some of the most important directions to be pursued in the remainder of the programme.

Deadline for applications: 15 October 2017.

British Mathematical Colloquium 2018

11–14 June 2018, St Andrews University

Website: tinyurl.com/ybuv2we7

This is advance notice of the BMC in 2018. Note that this is a different time of year from usual for the BMC. Plenary speakers are:

- Laura De Marco (Northwestern University)
- Irit Dinur (Weizmann Institute)
- Martin Hairer (Warwick)
- Nalini Joshi (Sydney)
- Paul Seymour (Princeton)
- Marcelo Viana (IMPA, Brazil)
- Julia Wolf (Bristol) will give a public lecture

There will be workshops on Algebra, Analysis and Probability, Dynamics, Combinatorics, and History of Mathematics. Three LMS Scheme 3 Networks will have meetings on the Thursday afternoon: North British Geometric Group Theory Seminar, North British Semigroups and Applications Network, and One Day Ergodic Theory Meetings.

More information, including booking arrangements, will be circulated in due course and further details will be added to the website.

BMC2018 is supported by the LMS, the Edinburgh Mathematical Society, the Glasgow Mathematical Journal Learning and Research Support Fund, and the Heilbronn Institute and is organised in partnership with the Clay Institute.

Society Meetings and Events

September 2017

7-8 LMS Prospects in Mathematics Meeting, Reading
18 LMS Midlands Regional Meeting, Loughborough
20 Popular Lectures, Birmingham

October 2017

12 Symmetry and Computation, LMS–IMA Meeting, London

November

2 BCS–FACS Evening Seminar: joint event with the LMS, London
10 Graduate Student Meeting, London
10 Society and Annual General Meeting, London

December 2017

13 SW & South Wales Regional Meeting, Cardiff

March 2018

2 Mary Cartwright Meeting, London

Calendar of Events

This calendar lists Society meetings and other mathematical events. Further information may be obtained from the appropriate LMS Newsletter whose number is given in brackets. A fuller list is given on the Society's website (lms.ac.uk/content/calendar). Please send updates and corrections to calendar@lms.ac.uk.

September 2017

1 Christopher Hooley and the Artin Conjecture: 50 Years On, Bristol (468)
4 Function Theory Meeting, De Morgan House, London (471)
4–8 European Study Groups with Industry, Warwick (468)
4–8 Variational Methods, New Optimisation Techniques and New Fast Numerical Algorithm, Cambridge (468)
5–9 British Science Festival, Brighton (471)
6–8 British Topology Meeting, Leicester (471)
7-8 LMS Prospects in Mathematics Meeting, Reading (472)
8–9 British Logic Colloquium 2017, Sussex (471)
10–15 Mathematics Education for the Future Decade, Balatonfüred, Hungary (460)
11–13 British Algebraic Geometry, Cambridge (471)
11–15 Diophantine Problems, Manchester (471)
11–15 Algebraic Topology of Manifolds LMS-CMI Research School, Oxford (468)
11–15 Introduction to Geometry, Dynamics, and Moduli in Low Dimensions LMS-CMI Research School, Warwick (468)
11–15 Scientific Computation and Differential Equations, Bath (466)
13-15 Ergodic Theory & Symbolic Dynamics, Queen Mary, University of London (472)
14–15 Heilbronn Annual Conference, Bristol (472)
15 Functor Categories for Groups, Lancaster University (472)
18 LMS Midlands Regional Meeting, Loughborough (472)
18–22 Extremal Combinatorics, Warwick (468)
20 LMS Popular Lectures, Birmingham (472)
24–29 Heidelberg Laureate Forum (465)

October 2017

2-4 Operator Theory, Reading (472)
2-6 Ice–Fluid Interaction, INI Workshop, Cambridge (470)
12 Symmetry and Computation, LMS-IMA Meeting, London (472)
18 Discrete Models and KPZ Universality, Durham University (472)
30-3 Nov Generative Models, Parameter Learning and Sparsity, Cambridge (471)

November 2017

1-2 Categorical Methods in Mirror Symmetry, University of Kent (472)
2 What is Mathematics Education, Really?, Lincoln (472)
2 BCS–FACS Evening Seminar: joint event with the LMS, London (472)
3 Combinatorics and Computation in Groups, ICMS, Edinburgh (472)
6-10 Ice–Structure Interaction INI Workhop, Cambridge (471)
7-8 Opportunities for the Future: Women in Mathematics, Bristol (471)
10 Graduate Student Meeting, London (472)
10 Society and Annual General Meeting, London (472)
11-12 MathsJam Annual Gathering, Yarnfield Park, Staffordshire (472)
13-17 Shape Analysis and Computational Anatomy INI Workshop, Cambridge (471)
29-1 Dec Form and Art, Toys, and Games INI Workshop, Cambridge (471)

December 2017

4-8 New Advances in Fano Manifolds, Cambridge (472)
4-8 Ice Fracture and Cracks INI Workshop, Cambridge (471)
11-15 Flows, Mappings and Shapes INI Workshop, Cambridge (472)
13 SW & South Wales Regional Meeting, Cardiff
18 Variational Approaches to Problems in Solid Mechanics, University of Warwick (472)
18-22 A Random Event in Honour of Ilya Goldsheid's 70th Birthday, Queen Mary, University of London (472)

January 2018

15-19 Theoretical and Algorithmic Underpinnings of Big Data INI Workshop, Cambridge (472)

April 2018

3-6 British Congress of Mathematics Education, Warwick (471)

June 2018

11-14 British Mathematical Colloquium 2018, University of St Andrews (472)