Engaged in Applications

A brief overview of the applications of number theory

Gaurish Korpal

The University of Arizona

October 07, 2022

Outline

1. Introduction

2. Applications
   - Elementary Number Theory
   - Arithmetic Geometry
   - Computational Number Theory
   - Algebraic Number Theory
   - Analytic Number Theory

3. Conclusion

A Mathematician's Apology

Godfrey Harold Hardy was the first non-Indian mathematician I read about because of his association with Srinivas Ramanujan, whose photo is at the beginning of every Indian mathematics school textbook. His ideas from the essay "A Mathematican's Apology" had a great impact on me during my formative years in mathematics (grades 8-10).

A Mathematician's Apology

Godfrey Harold Hardy was the first non-Indian mathematician I read about because of his association with Srinivas Ramanujan, whose photo is at the beginning of every Indian mathematics school textbook. His ideas from the essay "A Mathematican's Apology" had a great impact on me during my formative years in mathematics (grades 8-10).

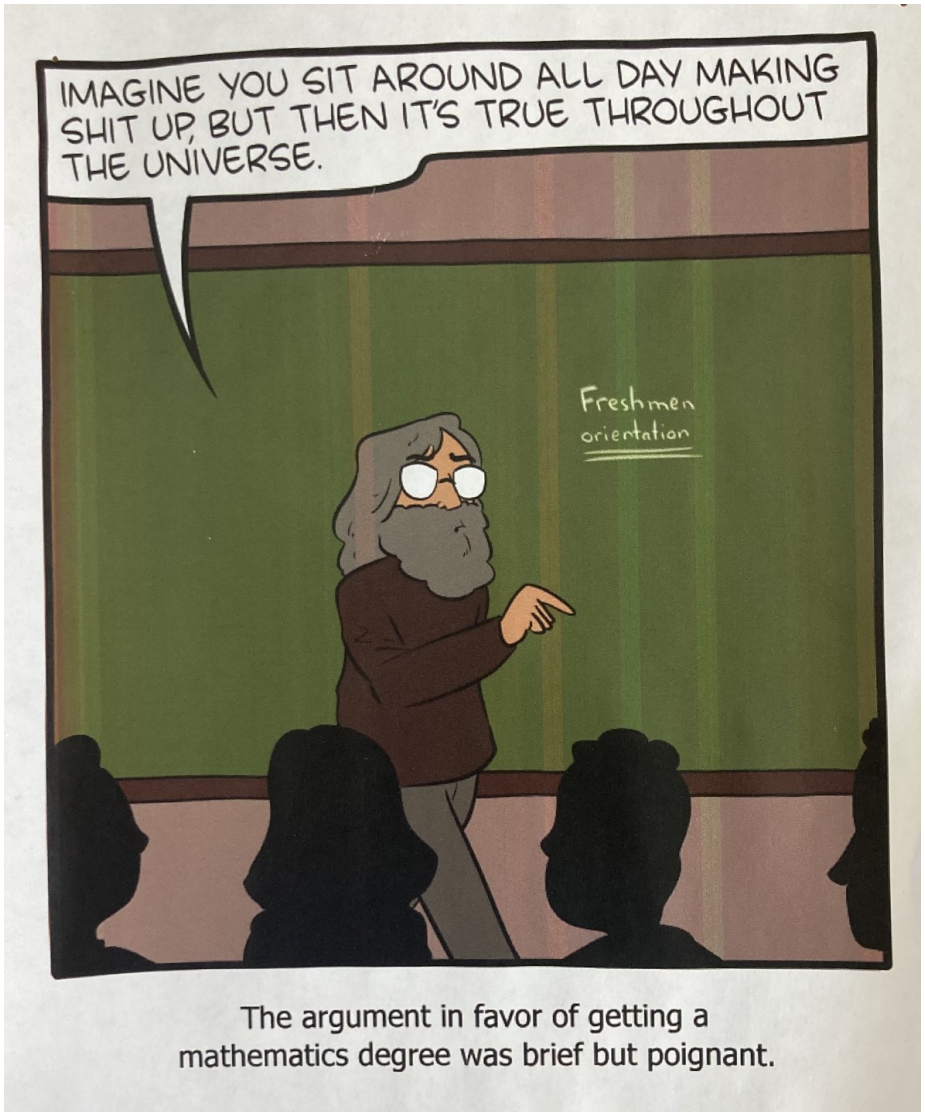
- A mathematician, like a painter or a poet, is a maker of patterns. If [the mathematician's] patterns are more permanent than theirs, it is because they are made with *ideas*.

A Mathematician's Apology

Godfrey Harold Hardy was the first non-Indian mathematician I read about because of his association with Srinivas Ramanujan, whose photo is at the beginning of every Indian mathematics school textbook. His ideas from the essay "A Mathematican's Apology" had a great impact on me during my formative years in mathematics (grades 8-10).

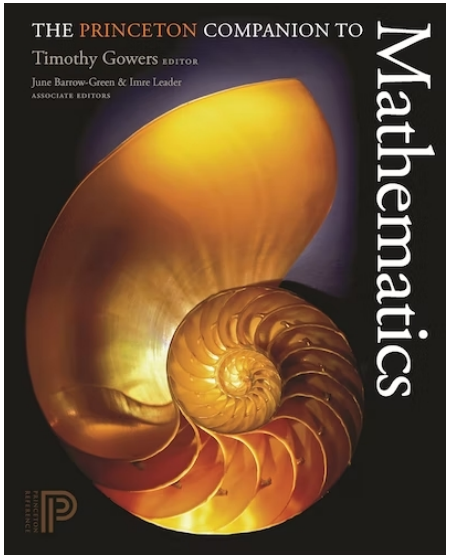
- A mathematician, like a painter or a poet, is a maker of patterns. If [the mathematician's] patterns are more permanent than theirs, it is because they are made with *ideas*.
- Pure mathematics is on the whole distinctly more useful than applied. [...] For what is useful above all is technique, and mathematical technique is taught mainly through pure mathematics.

The Past



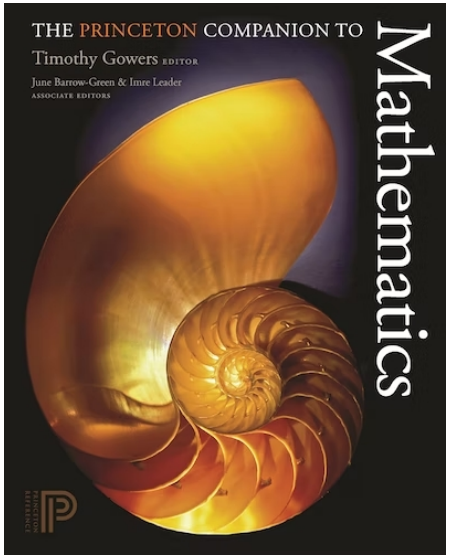
Credit: Cornell University Math Department Lounge, via Steven Strogatz, `https://twitter.com/stevenstrogatz/status/1577441222021320704`

The Princeton Companions

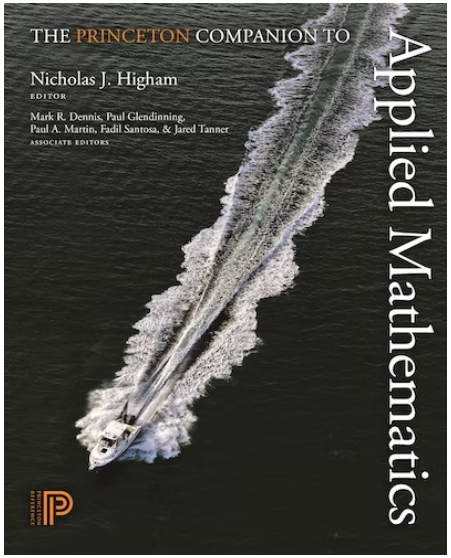


[...] there is no clear dividing line between pure and applied mathematics, and, just as a proper appreciation of modern mathematics requires some knowledge of its history, so a proper appreciation of pure mathematics requires some knowledge of applied mathematics and theoretical physics. – Timothy Gowers (Preface)

The Princeton Companions



[...] there is no clear dividing line between pure and applied mathematics, and, just as a proper appreciation of modern mathematics requires some knowledge of its history, so a proper appreciation of pure mathematics requires some knowledge of applied mathematics and theoretical physics. – Timothy Gowers (Preface)

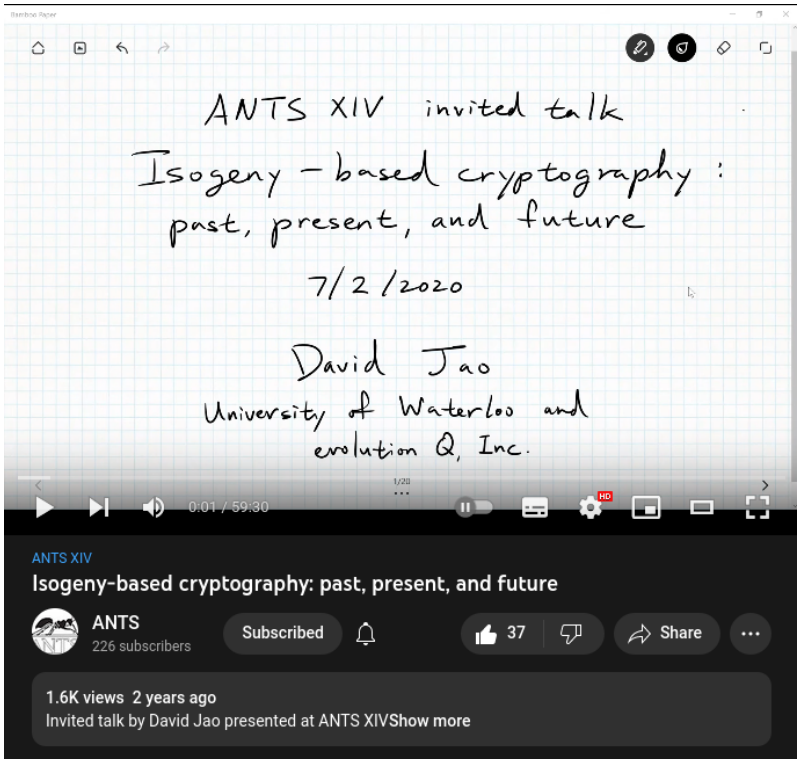


Applied mathematics is a large subject that interfaces with many other fields. Trying to define it is problematic. [...] The question of how applied mathematics compares with pure mathematics is often raised and has been discussed by many authors, sometimes in controversial terms. – Nicholas J. Higham (§I.1)

The Present

Credit: Saturday Morning Breakfast Cereal by Zach Weinersmith, "I bet you've engaged in... applications," `https://www.smbc-comics.com/comic/purity`

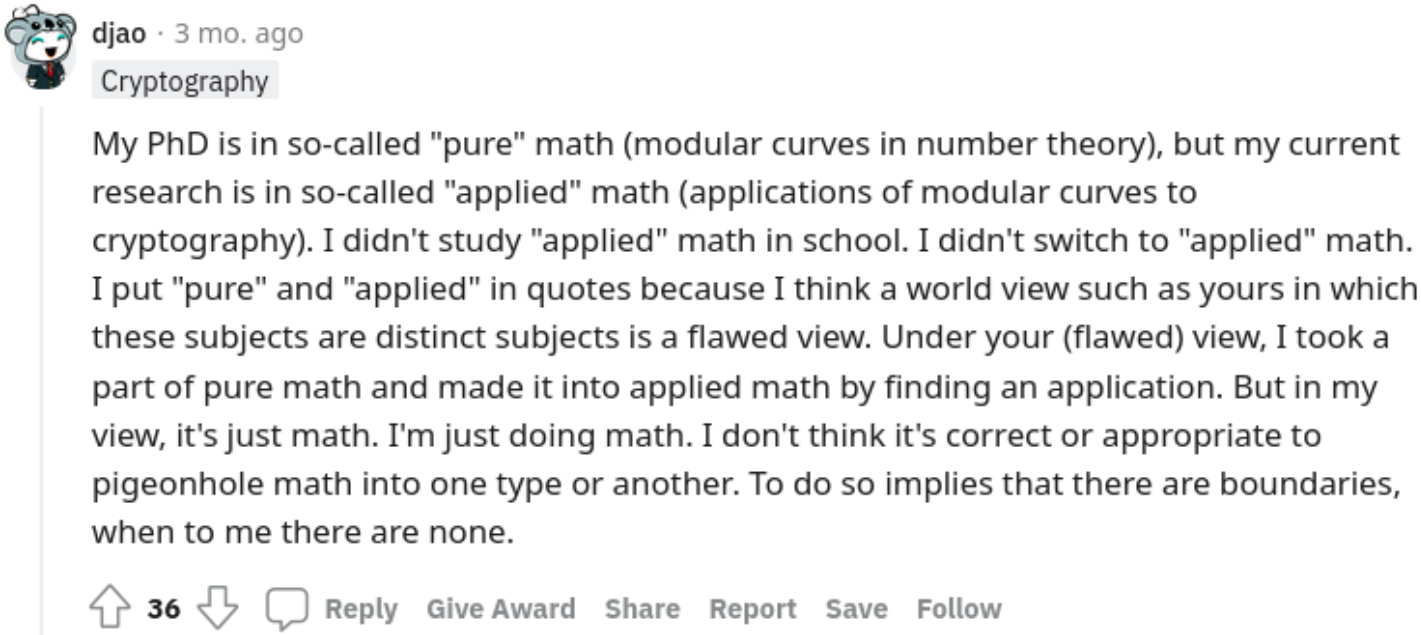
Mathematics Without Apologies[1]



David Jao works in the area of elliptic curve cryptography (classical, pairing-based, and isogeny-based) and related number-theoretic questions.
`uwaterloo.ca/news/global-impact/meet-man-protecting-your-secrets`

[1] Title of the book by **Michael Harris** about what pure mathematicians do, and why they do it. Looking beyond the conventional answers - for the sake of truth, beauty, and practical applications.

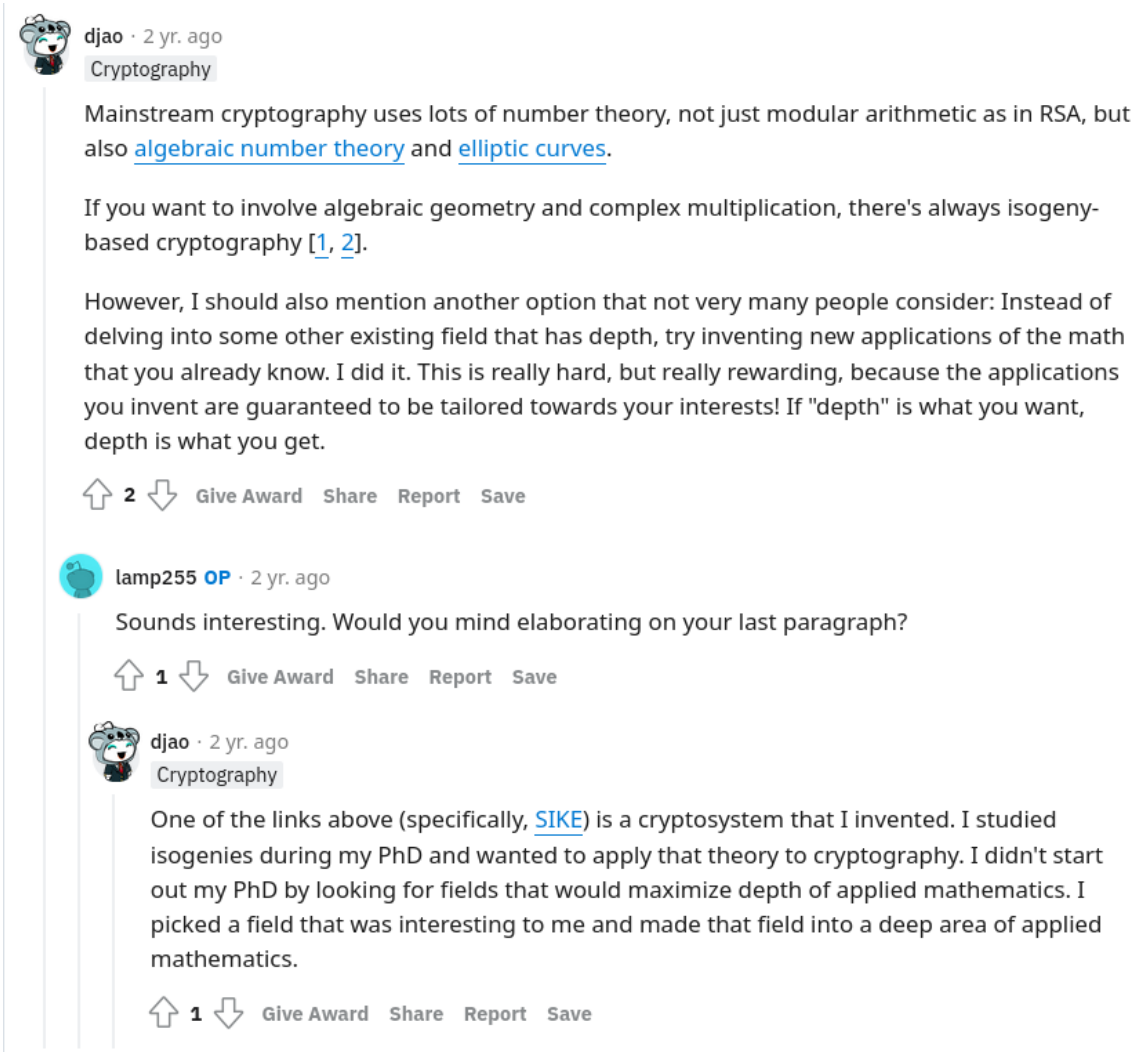
Mathematics Without Apologies[1]



Credit: Jao's comment on the Reddit post discussing the blog post "My two pieces of unsolicited advice for anyone about to start or currently in a PhD program is to (1) write daily and (2) work consistently/intentionally (Jun 19, 2022 MST)," `https://www.reddit.com/r/math/comments/vgbd4o/comment/id0tfmv/`

[1] Title of the book by **Michael Harris** about what pure mathematicians do, and why they do it. Looking beyond the conventional answers - for the sake of truth, beauty, and practical applications.

Mathematics Without Apologies[1]



djao · 2 yr. ago

Cryptography

Mainstream cryptography uses lots of number theory, not just modular arithmetic as in RSA, but also algebraic number theory and elliptic curves.

If you want to involve algebraic geometry and complex multiplication, there's always isogeny-based cryptography [1, 2].

However, I should also mention another option that not very many people consider: Instead of delving into some other existing field that has depth, try inventing new applications of the math that you already know. I did it. This is really hard, but really rewarding, because the applications you invent are guaranteed to be tailored towards your interests! If "depth" is what you want, depth is what you get.

2 Give Award Share Report Save

lamp255 OP · 2 yr. ago

Sounds interesting. Would you mind elaborating on your last paragraph?

1 Give Award Share Report Save

djao · 2 yr. ago

Cryptography

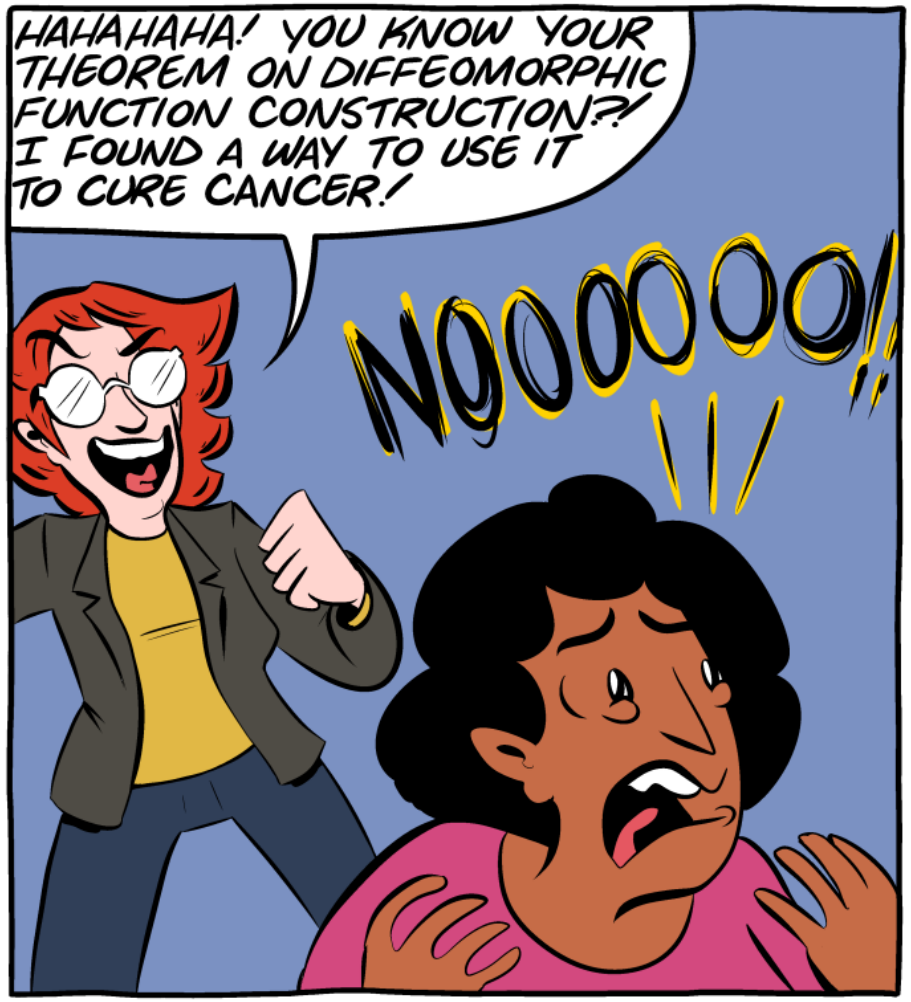
One of the links above (specifically, SIKE) is a cryptosystem that I invented. I studied isogenies during my PhD and wanted to apply that theory to cryptography. I didn't start out my PhD by looking for fields that would maximize depth of applied mathematics. I picked a field that was interesting to me and made that field into a deep area of applied mathematics.

1 Give Award Share Report Save

Credit: Jao's comment on the Reddit post discussing "What are the deepest areas of applied mathematics? (Sept 21, 2020 MST)," `https://www.reddit.com/r/math/comments/iwx5zb/comment/g6eez2d/`

[1] Title of the book by **Michael Harris** about what pure mathematicians do, and why they do it. Looking beyond the conventional answers - for the sake of truth, beauty, and practical applications.

The Future

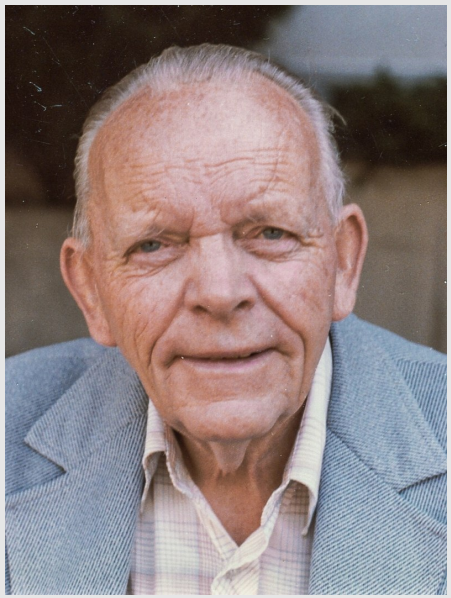


Funtime Activity:
Forcibly converting pure mathematicians into applied mathematicians.

Credit: Saturday Morning Breakfast Cereal by Zach Weinersmith, "At least tell me it only works in computer models!," `https://www.smbc-comics.com/comic/noooooooo`

Outline

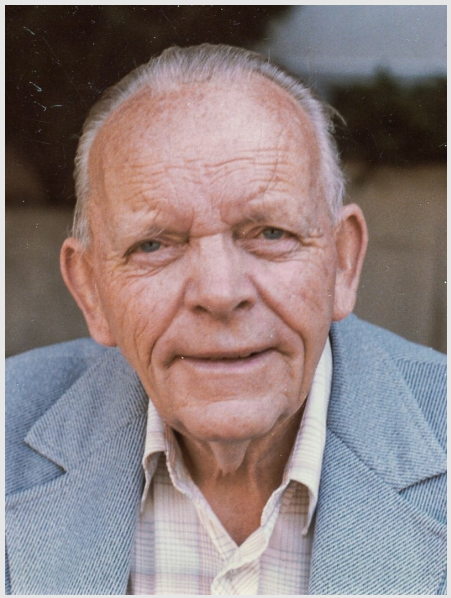
Modular Arithmetic



Derrick Henry "Dick" Lehmer, as an undergraduate, worked on Factor Stencils project with his father Derrick Norman Lehmer (DNL). While Dick and his father were working on the stencils, Emma Trotskaia who was a mathematics student studying DNL's courses, also assisted them. Later, after completing B.A. degree, Emma and Dick got married. Dick spent 1945-46 to help set up and operate the ENIAC computer. On some weekends the Lehmers used ENIAC to solve certain number theory problems using it as an electronic sieve. `https://mathshistory.st-andrews.ac.uk/Biographies/Lehmer_Derrick/`

[2] D. L. Johnson. "Generating and testing pseudo random numbers on the IBM Type 701". In: *Mathematics of Computation* 10.53 (1956), pp. 8–13. DOI: 10.1090/s0025-5718-1956-0076467-x.

Modular Arithmetic



Derrick Henry "Dick" Lehmer, as an undergraduate, worked on Factor Stencils project with his father Derrick Norman Lehmer (DNL). While Dick and his father were working on the stencils, Emma Trotskaia who was a mathematics student studying DNL's courses, also assisted them. Later, after completing B.A. degree, Emma and Dick got married. Dick spent 1945-46 to help set up and operate the ENIAC computer. On some weekends the Lehmers used ENIAC to solve certain number theory problems using it as an electronic sieve. `https://mathshistory.st-andrews.ac.uk/Biographies/Lehmer_Derrick/`

- **Linear congruential generator:** This was one of the first methods in the history of pseudorandom number generation introduced by Dick[2] at a conference at Harvard University in 1949. This method is still popular because of its simplicity.

[2] D. L. Johnson. "Generating and testing pseudo random numbers on the IBM Type 701". In: *Mathematics of Computation* 10.53 (1956), pp. 8–13. DOI: 10.1090/s0025-5718-1956-0076467-x.

Modular Arithmetic

Clifford Christopher Cocks, along with James Ellis and Malcolm Willaimson, invented public key cryptography within within six weeks of starting his new job at GCHQ in 1973. He didn't finish his PhD on elliptic curves with Bryan Birch because he "didn't want to spend three years just getting to the coal face." `https://chalkdustmagazine.com/interviews/clifford-cocks/`

[3] Clifford Cocks. "An Identity Based Encryption Scheme Based on Quadratic Residues". In: *Cryptography and Coding*. Springer Berlin Heidelberg, 2001, pp. 360–363. DOI: 10.1007/3-540-45325-3_32.

Modular Arithmetic

Clifford Christopher Cocks, along with James Ellis and Malcolm Willaimson, invented public key cryptography within within six weeks of starting his new job at GCHQ in 1973. He didn't finish his PhD on elliptic curves with Bryan Birch because he "didn't want to spend three years just getting to the coal face." `https://chalkdustmagazine.com/interviews/clifford-cocks/`

- **Rivest–Shamir–Adleman encryption:** A public-key encryption scheme based on prime factorization, equivalent to what was independently rediscovered in 1978 as the RSA algorithm.

[3] Clifford Cocks. "An Identity Based Encryption Scheme Based on Quadratic Residues". In: *Cryptography and Coding*. Springer Berlin Heidelberg, 2001, pp. 360–363. DOI: 10.1007/3-540-45325-3_32.

Modular Arithmetic

Clifford Christopher Cocks, along with James Ellis and Malcolm Willaimson, invented public key cryptography within within six weeks of starting his new job at GCHQ in 1973. He didn't finish his PhD on elliptic curves with Bryan Birch because he "didn't want to spend three years just getting to the coal face." `https://chalkdustmagazine.com/interviews/clifford-cocks/`

- **Rivest–Shamir–Adleman encryption:** A public-key encryption scheme based on prime factorization, equivalent to what was independently rediscovered in 1978 as the RSA algorithm.
- **Identity-based encryption:** A type of PKE based on quadratic residues[3] in which "identity" is used a public key. Not popular since a better pairing-based scheme was proposed soon after.

[3] Clifford Cocks. "An Identity Based Encryption Scheme Based on Quadratic Residues". In: *Cryptography and Coding*. Springer Berlin Heidelberg, 2001, pp. 360–363. DOI: 10.1007/3-540-45325-3_32.

Outline

Curves over Finite Fields

Valery Denisovich Goppa, in the period of 1977-1980, discovered a connection between the theory of algebraic curves over finite fields and the theory of q-ary codes which generalized the well known construction of Reed-Solomon codes. The RS codes use polynomials in one variable over finite fields, and Goppa's codes use rational functions on an algebraic curve. [T. Hiramatsu and G. Köhler, Coding Theory and Number Theory. Springer Netherlands, 2003 DOI: 10.1007/978-94-017-0305-5]

[4] V D Goppa. "Algebrico-Geometric codes". In: *Mathematics of the USSR-Izvestiya* 21.1 (Feb. 1983), pp. 75–91. DOI: 10.1070/im1983v021n01abeh001641.

Curves over Finite Fields

Valery Denisovich Goppa, in the period of 1977-1980, discovered a connection between the theory of algebraic curves over finite fields and the theory of q-ary codes which generalized the well known construction of Reed-Solomon codes. The RS codes use polynomials in one variable over finite fields, and Goppa's codes use rational functions on an algebraic curve. [T. Hiramatsu and G. Köhler, Coding Theory and Number Theory. Springer Netherlands, 2003 DOI: 10.1007/978-94-017-0305-5]

- **Algebraic geometry codes:** The geometric Goppa codes are defined using n points on a curve, and the vector space of equivalence classes of rational functions related to the function defining the curve[4].

[4] V D Goppa. "Algebrico-Geometric codes". In: *Mathematics of the USSR-Izvestiya* 21.1 (Feb. 1983), pp. 75–91. DOI: 10.1070/im1983v021n01abeh001641.

Curves with Many Points

Michael Anatolevich Tsfasman, in 1981, proved that there exist codes over the Gilbert–Varshamov bound. The preprint was smuggled through the iron curtain, which led to the gain in popularity of the algebraic geometry codes discovered by Goppa. "I have always dreamed of doing exactly pure mathematics [...] I have always been interested in the developments of ideas, not applications" `https://trv-science.ru/2016/02/o-bublikah-babushkah-i-korrektiruyushchikh-kodah/`

[5] M. A. Tsfasman, S. G. Vlăduts, and Th. Zink. "Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound". In: *Mathematische Nachrichten* 109.1 (1982), pp. 21–28. DOI: 10.1002/mana.19821090103.

Curves with Many Points

Michael Anatolevich Tsfasman, in 1981, proved that there exist codes over the Gilbert–Varshamov bound. The preprint was smuggled through the iron curtain, which led to the gain in popularity of the algebraic geometry codes discovered by Goppa. "I have always dreamed of doing exactly pure mathematics [...] I have always been interested in the developments of ideas, not applications" `https://trv-science.ru/2016/02/o-bublikah-babushkah-i-korrektiruyushchikh-kodah/`

- **Modular curve codes:** For 30 years after the publication of the Gilbert–Varshamov Bound, no family of codes had been demonstrated to exceed this bound until such a family of algebraic geometry codes was shown to exist using modular curves with many rational points[5].

[5] M. A. Tsfasman, S. G. Vlăduts, and Th. Zink. "Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound". In: *Mathematische Nachrichten* 109.1 (1982), pp. 21–28. DOI: 10.1002/mana.19821090103.

Elliptic and Hyperelliptic Curve

Neal I. Koblitz, in late 1984, received a one-page description from Hendrik Lenstra of his method for factoring large integers using elliptic curves. This was the first time that elliptic curves had been used in cryptography. Shortly after, while in USSR, it occurred to him that elliptic curves can be used to construct systems based on the problem of finding logarithms on the curve. ["Cryptography." In: Random Curves. Springer Berlin Heidelberg, pp. 297-329, 2008]

[6] Neal Koblitz. "Elliptic curve cryptosystems". In: *Math. of Computation* 48.177 (1987), pp. 203–209. DOI: 10.1090/s0025-5718-1987-0866109-5.

[7] Neal Koblitz. "Hyperelliptic cryptosystems". In: *Journal of Cryptology* 1.3 (Oct. 1989), pp. 139–150. DOI: 10.1007/bf02252872.

Elliptic and Hyperelliptic Curve

Neal I. Koblitz, in late 1984, received a one-page description from Hendrik Lenstra of his method for factoring large integers using elliptic curves. This was the first time that elliptic curves had been used in cryptography. Shortly after, while in USSR, it occurred to him that elliptic curves can be used to construct systems based on the problem of finding logarithms on the curve. ["Cryptography." In: Random Curves. Springer Berlin Heidelberg, pp. 297-329, 2008]

- **Elliptic curve cryptography:** A PKE scheme based on the discrete-log problem for the group of points of an elliptic curve over finite field[6].

[6] Neal Koblitz. "Elliptic curve cryptosystems". In: *Math. of Computation* 48.177 (1987), pp. 203–209. DOI: 10.1090/s0025-5718-1987-0866109-5.

[7] Neal Koblitz. "Hyperelliptic cryptosystems". In: *Journal of Cryptology* 1.3 (Oct. 1989), pp. 139–150. DOI: 10.1007/bf02252872.

Elliptic and Hyperelliptic Curve

Neal I. Koblitz, in late 1984, received a one-page description from Hendrik Lenstra of his method for factoring large integers using elliptic curves. This was the first time that elliptic curves had been used in cryptography. Shortly after, while in USSR, it occurred to him that elliptic curves can be used to construct systems based on the problem of finding logarithms on the curve. ["Cryptography." In: Random Curves. Springer Berlin Heidelberg, pp. 297-329, 2008]

- **Elliptic curve cryptography:** A PKE scheme based on the discrete-log problem for the group of points of an elliptic curve over finite field[6].
- **Hyperelliptic curve cryptography:** A PKE scheme based on the discrete-log problem for the divisor class group of a hyperelliptic curve over a finite field[7].

[6] Neal Koblitz. "Elliptic curve cryptosystems". In: *Math. of Computation* 48.177 (1987), pp. 203–209. DOI: 10.1090/s0025-5718-1987-0866109-5.

[7] Neal Koblitz. "Hyperelliptic cryptosystems". In: *Journal of Cryptology* 1.3 (Oct. 1989), pp. 139–150. DOI: 10.1007/bf02252872.

Elliptic Curves

Jean-Marc Couveignes introduced the Hard Homogeneous Spaces framework in 1997, but his work was rejected at CRYPTO97 and stayed unpublished. In 2006, Alexander Rostovtsev and Anton Stolbunov independently rediscovered Couveignes ideas, suggesting isogeny-based Diffie–Hellman as a quantum-resistant primitive. Later, in 2018, adapting the CRS scheme to supersingular elliptic curves, a more efficient non-interactive key exchange cryptosystem CSIDH was proposed. `https://csidh.isogeny.org/`

[8] Jean-Marc Couveignes. *Hard Homogeneous Spaces*. Cryptology ePrint Archive, Paper 2006/291. `https://eprint.iacr.org/2006/291`. 2006.

Elliptic Curves

Jean-Marc Couveignes introduced the Hard Homogeneous Spaces framework in 1997, but his work was rejected at CRYPTO97 and stayed unpublished. In 2006, Alexander Rostovtsev and Anton Stolbunov independently rediscovered Couveignes ideas, suggesting isogeny-based Diffie–Hellman as a quantum-resistant primitive. Later, in 2018, adapting the CRS scheme to supersingular elliptic curves, a more efficient non-interactive key exchange cryptosystem CSIDH was proposed. `https://csidh.isogeny.org/`

- **Couveignes-Rostovtsev-Stolbunov key exhange:** A key exchange scheme based on the commutative action of isogenies on ordinary elliptic curves[8]. The CRS system closely resembles the Diffie-Hellman key exchange.

[8] Jean-Marc Couveignes. *Hard Homogeneous Spaces*. Cryptology ePrint Archive, Paper 2006/291. `https://eprint.iacr.org/2006/291`. 2006.

Elliptic Curve

Antoine Joux, together with Dan Boneh and Matt Franklin, received the 2013 Gödel prize for his work on pairing-based cryptography. His PhD advisor Jacques Stern inspired him to take the path of research and cryptography. Stern began his career a mathematician before becoming interested in computer science and moving on to cryptology, winning CNRS Gold Medal for 2006. [A. Joux, Algorithmic cryptanalysis. CRC Press, 2009.]

[9] Antoine Joux. "A One Round Protocol for Tripartite Diffie–Hellman". In: *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2000, pp. 385–393. DOI: 10.1007/10722028_23.

Elliptic Curve

Antoine Joux, together with Dan Boneh and Matt Franklin, received the 2013 Gödel prize for his work on pairing-based cryptography. His PhD advisor Jacques Stern inspired him to take the path of research and cryptography. Stern began his career a mathematician before becoming interested in computer science and moving on to cryptology, winning CNRS Gold Medal for 2006. [A. Joux, Algorithmic cryptanalysis. CRC Press, 2009.]

- **Pairing-based cryptography:** The (modified) Weil and Tate pairings were initially used in the cryptanalysis of ECC. However, Joux[9] was able to use them to generalize the two-party key agreement of Diffie and Hellman to a multi-party key exchange. This soon led to a practical scheme for identity-based encryption.

[9] Antoine Joux. "A One Round Protocol for Tripartite Diffie–Hellman". In: *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2000, pp. 385–393. DOI: 10.1007/10722028_23.

Elliptic Curves

Kristin Estella Lauter, in 1996, developed and taught a new math course on coding theory and cryptography at the University of Michigan. This course attracted many students from engineering. Getting to know these students and their professors in engineering caused her to become interested in the practical applications which led her to apply for a job in cryptography at MSR in 1999. https://www.siam.org/Portals/0/StudentPrograms/ThinkingofaCareer/brochure.pdf

[10] Denis X. Charles, Kristin E. Lauter, and Eyal Z. Goren. "Cryptographic Hash Functions from Expander Graphs". In: *Journal of Cryptology* 22.1 (Sept. 2007), pp. 93–113. DOI: 10.1007/s00145-007-9002-x.

Elliptic Curves

Kristin Estella Lauter, in 1996, developed and taught a new math course on coding theory and cryptography at the University of Michigan. This course attracted many students from engineering. Getting to know these students and their professors in engineering caused her to become interested in the practical applications which led her to apply for a job in cryptography at MSR in 1999. `https://www.siam.org/Portals/0/StudentPrograms/ThinkingofaCareer/brochure.pdf`

- **Charles-Goren-Lauter hash function:** A cryptographic hash function based on the Ramanujan graph of supersingular elliptic curves[10]. This is not considered secure anymore, but it paved path for many other isogeny-based cryptography schemes.

[10] Denis X. Charles, Kristin E. Lauter, and Eyal Z. Goren. "Cryptographic Hash Functions from Expander Graphs". In: *Journal of Cryptology* 22.1 (Sept. 2007), pp. 93–113. DOI: 10.1007/s00145-007-9002-x.

Outline

Elliptic Curve

Victor Saul Miller and Koblitz both came up with the idea of ECC simultaneously and independently of one another. They both had similar mathematical training - Miller wrote his thesis on elliptic curves under Barry Mazur at about the same time as Koblitz wrote his thesis on p-adic analysis under Nicholas Katz. `https://www.iacr.org/conferences/eurocrypt2007/slides/s14t1.pdf`

[11] Victor S. Miller. "Short Programs for Functions on Curves." IBM Thomas J. Watson Research Center (available at `https://crypto.stanford.edu/miller/`), 1986

Elliptic Curve

Victor Saul Miller and Koblitz both came up with the idea of ECC simultaneously and independently of one another. They both had similar mathematical training - Miller wrote his thesis on elliptic curves under Barry Mazur at about the same time as Koblitz wrote his thesis on p-adic analysis under Nicholas Katz. `https://www.iacr.org/conferences/eurocrypt2007/slides/s14t1.pdf`

- **Miller's algorithm:** In September 1985, Miller found an efficient algorithm (linear in the size of the input) for evaluating the Weil pairing on an elliptic curve, and wrote it up as a short note which was never published though widely distributed and cited[11]. This algorithm was initially used to attack certain elliptic curve cryptosystems, but it later became the core of pairing-based cryptosystems.

[11] Victor S. Miller. "Short Programs for Functions on Curves." IBM Thomas J. Watson Research Center (available at `https://crypto.stanford.edu/miller/`), 1986

Lattice

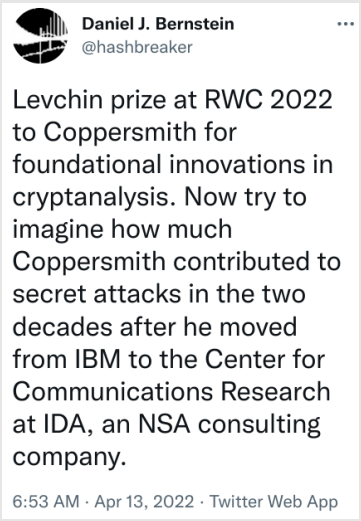
Don Coppersmith received his Ph.D. in Lie groups from Harvard University in 1977. He was a Putnam Fellow each year from 1968–1971, becoming the first four-time Putnam Fellow in history.

[12] Don Coppersmith. "Finding a Small Root of a Univariate Modular Equation." In: EUROCRYPT '96. DOI: 10.1007/3-540-68339-9_14.

[13] Don Coppersmith. "Finding a Small Root of a Bivariate Integer Equation Factoring with High Bits Known." In: EUROCRYPT '96. DOI: 10.1007/3-540-68339-9_16.

Lattice

Don Coppersmith received his Ph.D. in Lie groups from Harvard University in 1977. He was a Putnam Fellow each year from 1968–1971, becoming the first four-time Putnam Fellow in history.



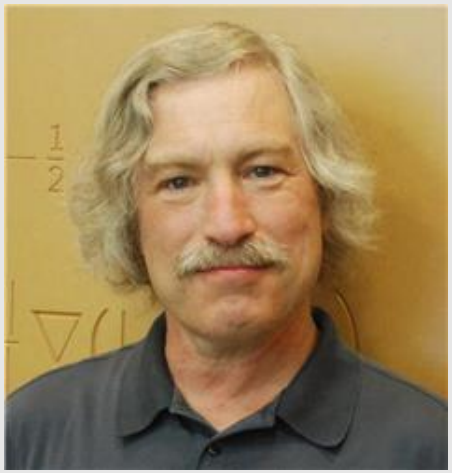
- **Coppersmith method:** It's a method to find small integer zeroes of univariate[12] or bivariate[13] polynomials modulo a given integer. This method is mainly used in attacks on RSA when parts of the secret key are known.

[12] Don Coppersmith. "Finding a Small Root of a Univariate Modular Equation." In: EUROCRYPT '96. DOI: 10.1007/3-540-68339-9_14.

[13] Don Coppersmith. "Finding a Small Root of a Bivariate Integer Equation Factoring with High Bits Known." In: EUROCRYPT '96. DOI: 10.1007/3-540-68339-9_16.

Outline

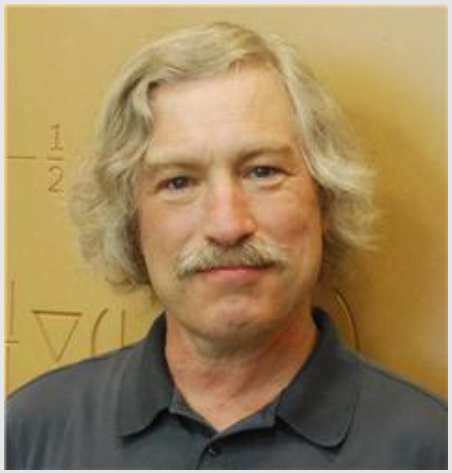
Ideal Lattice



Jeffrey Ezra Hoffstein, had a child in 1992, after which he realized that applications that led to a lot of money could have their point. In 1994, he heard a talk by Dorian Goldfeld that connected some of his previous result to cryptography. In 1996, with fellow Brown mathematicians Jill Pipher and Joseph Silverman, he founded NTRU Cryptosystems, Inc. to market their cryptographic algorithms, NTRUEncrypt and NTRUSign. `https://sinews.siam.org/About-the-Author/an-interview-with-jeff-hoffstein`

[14] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. "NTRU: A ring-based public key cryptosystem". In: *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 1998, pp. 267–288. DOI: 10.1007/bfb0054868.

Ideal Lattice



Jeffrey Ezra Hoffstein, had a child in 1992, after which he realized that applications that led to a lot of money could have their point. In 1994, he heard a talk by Dorian Goldfeld that connected some of his previous result to cryptography. In 1996, with fellow Brown mathematicians Jill Pipher and Joseph Silverman, he founded NTRU Cryptosystems, Inc. to market their cryptographic algorithms, NTRUEncrypt and NTRUSign. `https://sinews.siam.org/About-the-Author/an-interview-with-jeff-hoffstein`

- **NTRU:** A public-key cryptosystem based on lattices in high dimentions, which is more efficient and lightweight than other public-key cryptosystems based on factoring large integers (RSA) or the discrete log problem (ECC)[14]. The name "NTRU" was originally derived from the pun *Number Theorists 'R' Us* or, alternatively, stood for *Number Theory Research Unit*.

[14] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. "NTRU: A ring-based public key cryptosystem". In: *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 1998, pp. 267–288. DOI: 10.1007/bfb0054868.

Outline

Modular Forms

Florence Jessie MacWilliams, in 1958, joined Bell Labs as a computer programmer. There she became interested in coding theory after listening to a talk by R. C. Bose, and wanted to become a member of the technical staff which required a PhD. Therefore, in 1961, she returned to Harvard for a year and wrote thesis on combinatorial results in coding theory with Andrew Gleason. `https://awm-math.org/awards/noether-lectures/noether-lectures-1980/`

[15] `https://www.ias.ac.in/article/fulltext/reso/010/01/0002-0003`

[16] E. Berlekamp, F. MacWilliams, and N. Sloane. "Gleason's theorem on self-dual codes". In: *IEEE Transactions on Information Theory* 18.3 (May 1972), pp. 409–414. DOI: 10.1109/tit.1972.1054817.

Modular Forms

Florence Jessie MacWilliams, in 1958, joined Bell Labs as a computer programmer. There she became interested in coding theory after listening to a talk by R. C. Bose, and wanted to become a member of the technical staff which required a PhD. Therefore, in 1961, she returned to Harvard for a year and wrote thesis on combinatorial results in coding theory with Andrew Gleason. `https://awm-math.org/awards/noether-lectures/noether-lectures-1980/`

- **Self-dual codes:** In 1968, Jessie's daughter Anne, who was a student of John Thompson, wrote to Jessie that J H Conway had just discovered a new simple group that was connected with a certain packing of spheres in twenty-four dimensions[15]. This led to a chain of events resulting in the discovery of link between coding theory and theta functions[16].

[15] `https://www.ias.ac.in/article/fulltext/reso/010/01/0002-0003`

[16] E. Berlekamp, F. MacWilliams, and N. Sloane. "Gleason's theorem on self-dual codes". In: *IEEE Transactions on Information Theory* 18.3 (May 1972), pp. 409–414. DOI: 10.1109/tit.1972.1054817.

Exponential sums

Nikolai Mikhailovich Korobov became interested in analytic number theory after meeting A.O. Gelfond at college. After the second world war, he completed his PhD working with A.O. Gelfond. He contributed to the results about fractional distributions, estimations of trigonometric sums, and the application of evaluated estimates to different problems of analytical numbers theory and approximate computation of multiple integrals. `http://poivs.tsput.ru/conf/international/XV/index_en.php`

[17] N. M. Korobov. *Exponential Sums and their Applications*. Springer Netherlands, 1992. DOI: 10.1007/978-94-015-8032-8.

Exponential sums

Nikolai Mikhailovich Korobov became interested in analytic number theory after meeting A.O. Gelfond at college. After the second world war, he completed his PhD working with A.O. Gelfond. He contributed to the results about fractional distributions, estimations of trigonometric sums, and the application of evaluated estimates to different problems of analytical numbers theory and approximate computation of multiple integrals. `http://poivs.tsput.ru/conf/international/XV/index_en.php`

- **Quasi-Monte Carlo:** QMC methods are deterministic versions of the Monte Carlo methods invented in the 1940s by von Neumann and Ulam working at the Los Alamos Lab. The systematic research on QMC methods began in the late 1950s with the work of Korobov[17]. QMC methods outperform MC methods in many challenging problems arising in computational finance, computational physics, and computer graphics.

[17] N. M. Korobov. *Exponential Sums and their Applications*. Springer Netherlands, 1992. DOI: 10.1007/978-94-015-8032-8.

Exponential sums

Yuan Wang, while an undergraduate student at Chekiang University, fell in love with analytic number theory and gave a series of lectures to the graduate seminar based on Ingham's book "The distribution of prime numbers." He graduated in 1952 and was assigned by the government to the number theory section in the Institute of Mathematics at the Academia Sinica where he worked under Hua Loo-Keng. He is best known for his contributions to the Goldbach conjecture. `https://mathshistory.st-andrews.ac.uk/Biographies/Wang_Yuan/`

[18] Kai-Tai Fang, Yuan Wang, and Peter M. Bentler. "Some Applications of Number-Theoretic Methods in Statistics". In: *Statistical Science* 9.3 (Aug. 1994). DOI: 10.1214/ss/1177010392.

Exponential sums

Yuan Wang, while an undergraduate student at Chekiang University, fell in love with analytic number theory and gave a series of lectures to the graduate seminar based on Ingham's book "The distribution of prime numbers." He graduated in 1952 and was assigned by the government to the number theory section in the Institute of Mathematics at the Academia Sinica where he worked under Hua Loo-Keng. He is best known for his contributions to the Goldbach conjecture. `https://mathshistory.st-andrews.ac.uk/Biographies/Wang_Yuan/`

- **Design of Experiments:** In response to a Chinese industrial agency's proposed problems of experimental designs the statistician Kai-Tai Fang collaborated with Wang to develop a "uniform design" using the high-dimensional combinatorial designs for numerical integration on the unit cube[18].

[18] Kai-Tai Fang, Yuan Wang, and Peter M. Bentler. "Some Applications of Number-Theoretic Methods in Statistics". In: *Statistical Science* 9.3 (Aug. 1994). DOI: 10.1214/ss/1177010392.

Exponential sums

Gilles Lachaud got interested in information theory after reading Tsfasman's article dealing with application of modular functions to the theory of Goppa codes. His work on codes and curves over finite fields started with questions where he could use his expertise in exponential sums, Kloostermann sums, Eisenstein sums, and so on. In 1987 he started organizing the biennial conference now called AGC^{2}T (Arithmetic, Geometry, Cryptography, and Coding Theory). `https://arxiv.org/abs/2004.03263`

[19] Gilles Lachaud. "Artin-Schreier curves, exponential sums, and coding theory". In: *Theoretical Computer Science* 94.2 (Mar. 1992), pp. 295–310. DOI: 10.1016/0304-3975(92)90040-m.

Exponential sums

Gilles Lachaud got interested in information theory after reading Tsfasman's article dealing with application of modular functions to the theory of Goppa codes. His work on codes and curves over finite fields started with questions where he could use his expertise in exponential sums, Kloostermann sums, Eisenstein sums, and so on. In 1987 he started organizing the biennial conference now called AGC^{2}T (Arithmetic, Geometry, Cryptography, and Coding Theory). `https://arxiv.org/abs/2004.03263`

- **Kloostermann Code:** An error-correcting code based on the connection between exponential sums and the number of points of curves, which is also dual of Melas code[19].

[19] Gilles Lachaud. "Artin-Schreier curves, exponential sums, and coding theory". In: *Theoretical Computer Science* 94.2 (Mar. 1992), pp. 295–310. DOI: 10.1016/0304-3975(92)90040-m.

Outline

1 Introduction

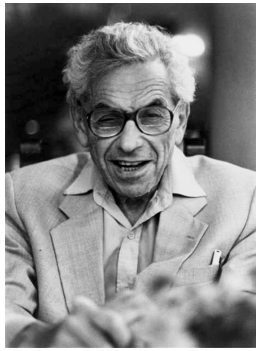
2 Applications
- Elementary Number Theory
- Arithmetic Geometry
- Computational Number Theory
- Algebraic Number Theory
- Analytic Number Theory

3 Conclusion

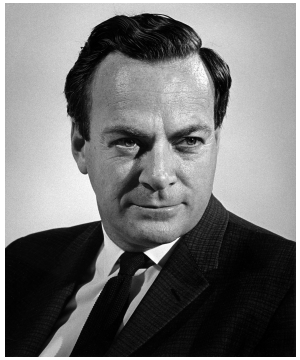
Battles, Wars, and Mathematics

All mathematics leads, doesn't it, sooner or later, to some kind of human suffering. –Against the Day[20], p. 54.

Fourier's well-known heat equation was developed in 1822 hired by Napoleon to increase a cannon's rate of fire, which was limited by overheating.



In 1943, Stanisław Ulam invited Erdős to join the Manhattan Project, but the invitation was withdrawn when Erdős expressed a desire to return to Hungary after the war.



"[John] von Neumann gave me an interesting idea: that you don't have to be responsible for the world that you're in. [...] It's made me a very happy man ever since."– Feynman

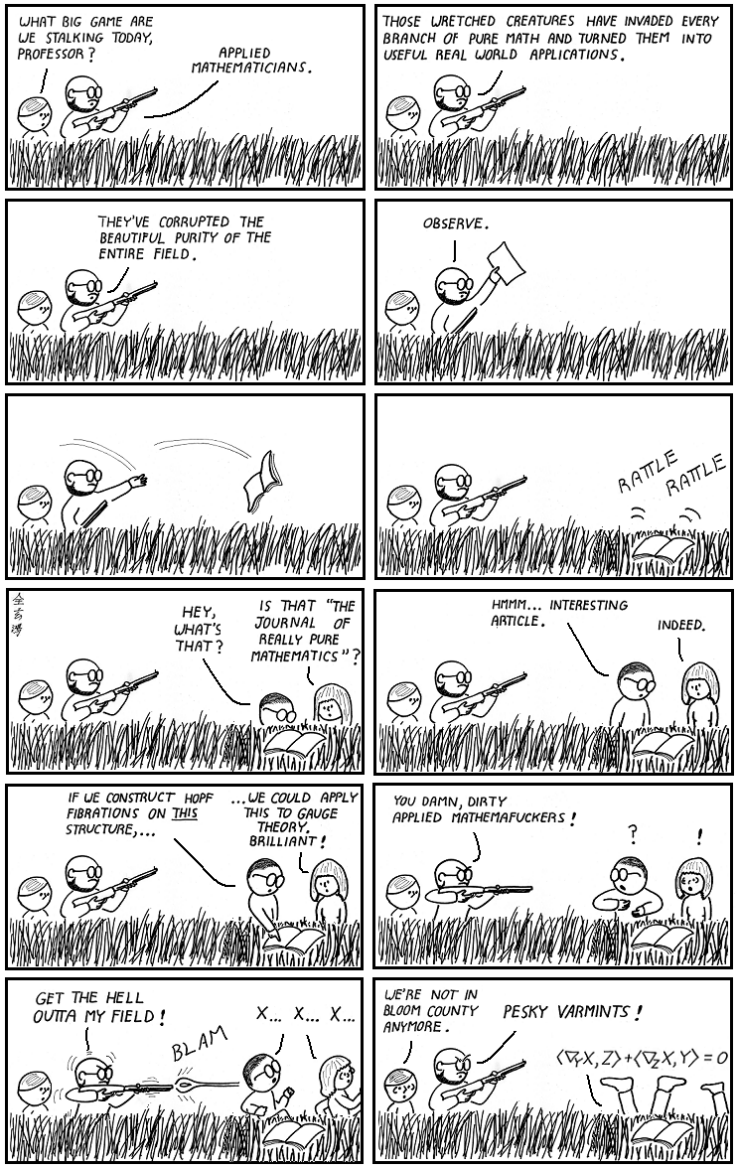
Immediately after Pearl Harbor, the US Navy started recruiting college seniors from the Seven Sisters schools, and some other women's colleges. Edith Reynolds White (center) worked in the WAVES unit responsible for cracking Japanese codes.

In 1958, Alexander Grothendieck was appointed a research professor at the IHÉS and remained there until 1970, when, driven by personal and political convictions, he left following a dispute over military funding.

In World War II the chief Allied powers were Great Britain, France, the Soviet Union, the United States, and China. – `Britannica`

[20] An historical novel by Thomas Pynchon, about the time just after World War I. Pychon modeled the major character Yashmenn Halfcourt after Sofia Kovalevskaya. `https://en.wikipedia.org/wiki/Against_the_Day`

Thank You!



Credit: Abstruse Goose.
`abstrusegoose.com/105`