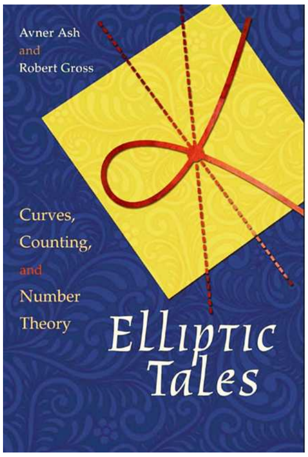
Book Reviews

Elliptic Tales: Curves, Counting and Number Theory

Avner Ash and Robert Gross
Princeton University Press, 2012, ISBN: 978-0-691-15119-9
Distributed in Australia by Footprint Books

An intriguing side-effect of the Clay Millennium Prize Problems is the rise in public awareness of and interest in what mathematicians actually do. For example, there was wide press coverage of the rejection by Perelman of the million dollar award for his solution of the Poincaré Conjecture, and numerous publications aimed at a nonspecialist audience and dealing with the Riemann Hypothesis have appeared. *Elliptic Tales* will similarly popularise the first Clay Prize Problem, namely the Birch and Swinnerton-Dyer (BS-D) conjecture.

An elliptic curve over a field $\mathbb{F}$ is the solution set $E(A, B, \mathbb{F})$ in $\mathbb{F}^2$ of an equation $y^2 = x^3 + Ax + B$, where A and B are integers and the equation has nonzero discriminant $\Delta = -16(4A^3 + 27B^2)$. If $\mathbb{F}$ has characteristic p, then we interpret A and B modulo p. The nonzero discriminant condition is equivalent to the cubic $x^3 + Ax + B$ having no multiple roots, and in case $\mathbb{F} = \mathbb{C}$, equivalent to the curve being smooth.



Apart from their intrinsic algebraic and geometric interest, elliptic curves have important applications to cryptography, factoring large integers, proving primality, and the congruent number problem. Elliptic curve theory was crucial in the proof of Fermat's Last Theorem.

The BS-D conjecture is a surprising relationship between the solutions of $E(A, B, \mathbb{Q})$ and those of $E(A, B, \mathbb{F}_p)$ for the prime fields $\mathbb{F}_p$. More precisely, it states that the number of independent solutions of infinite order in $E(A, B, \mathbb{Q})$ is a certain average over all primes p of N_p/p, where $N_p = |E(A, B, \mathbb{F}_p)|$.

The problem is best considered in the context of the homogeneous polynomial equation $y^2z = x^3 + Axz^2 + Bz^3$ in the projective plane over the algebraic closure of $\mathbb{F}$, so that the point at infinity is always a solution.

For any field $\mathbb{F}$, addition can be defined on the set $E(A, B, \mathbb{F})$ to give it the structure of a finitely generated Abelian group with identity the point at infinity. When $\mathbb{F} = \mathbb{Q}$ this group is a direct sum $T \oplus H$, where T is finite and $H \cong \mathbb{Z}^r$ is a free Abelian group of rank r. The torsion part T is well known so the interest lies in the rank r of the torsion-free component H of $E(A, B, \mathbb{Q})$. This r is the maximum number of solutions of infinite order that are linearly independent.

In the case of prime fields, we must differentiate between the finitely many singular primes, that is, the primes p which divide the discriminant Δ, and the rest. For nonsingular p it is known that regardless of A and B, N_p is bounded by

$$p + 1 - 2\sqrt{p} < N_p < p + 1 + 2\sqrt{p}.$$

To estimate the average size of N_p/p, one defines the Hasse–Weil L-function of the elliptic curves $E = E(A, B, \mathbb{F}_p)$ by $L(E, s) = \prod_p (f(p, s))^{-1}$, where s is a complex variable and

$$f(p, s) = 1 - \frac{1 + p - N_p}{p^s} + \frac{p}{p^{2s}}$$

if p is nonsingular, and equal to a certain polynomial in p^{-s} otherwise.

The product $L(E, s)$ does not converge at $s = 1$, but formally, $L(E, 1)$ is asymptotic to $\prod_p N_p/p$ as p increases, and it was this behaviour that led Birch and Swinnerton-Dyer to make their conjecture. In fact, $L(E, s)$ converges absolutely and uniformly on the complex half-plane $\{s \in \mathbb{C}\colon \mathrm{Re}(s) > 3/2\}$ and hence, by the recently proved result that elliptic curves are modular, can be analytically continued to the whole of $\mathbb{C}$. This in turn implies that the entire function $L(E, s)$ has a Taylor series expansion at $s = 1$ of the form

$$L(E, s) = c(s - 1)^\rho + \text{higher order terms},$$

where $c \neq 0$. The positive integer ρ is called the analytic rank of E. The BS-D conjecture is that the analytic rank $\rho = r$, where r is the algebraic rank of $E(A, B, \mathbb{Q})$.

Since Bryan Birch and Peter Swinnerton-Dyer made their conjecture in 1965, much research and numerical experimentation have been devoted to the problem. The BS-D conjecture holds for $r = 0$ or 1 and probability arguments show that a random elliptic curve has algebraic rank 0 or 1 almost surely. Apart from this however, positive results remain sparse. It is difficult to construct elliptic curves of large algebraic rank. For example, the largest integer r for which an elliptic curve is known to have rank r is 19, and A and B in that example are of the order of 10^{50}. The situation with analytic rank is even more dire. No elliptic curve is known to have analytic rank greater than 3. Work continues on the problem and on related results in number theory.

Ash and Gross painstakingly explain these results in a manner intelligible to a reader with a basic knowledge of calculus and linear algebra. Beginning with the equation of a curve in the Euclidean plane represented by a real polynomial in two indeterminates, they show how the solution of polynomial equations requires firstly extending the domain to the complex numbers and then to the projective plane. The authors introduce enough algebraic geometry to define intersection multiplicities and prove Bézout's theorem on the intersection of curves. They then concentrate on cubic equations, and their prototype, the elliptic curves. They derive the group theoretic properties of $E(A, B, \mathbb{F})$ both geometrically and algebraically. Throughout, they present numerous worked examples.

The authors then turn to the analytic aspects of the theory, introducing generating functions, Dirichlet series, Euler products and analytic continuation. This culminates in the Hasse–Weil L-function and finally the BS-D conjecture.

The argument is presented in an informal, sometimes playful, manner that will appeal to the mathematical amateur. Furthermore, the minimal prerequisites and clear writing make this book a suitable choice for a postgraduate student seminar.

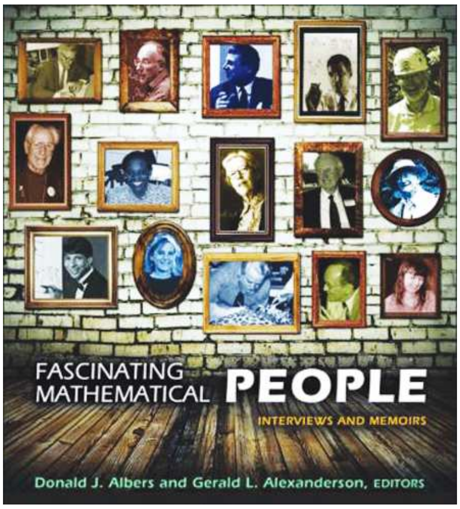
Phill Schultz
School of Mathematics and Statistics, The University of Western Australia.
Email: phill.schultz@uwa.edu.au

◇ ◇ ◇ ◇ ◇ ◇

Fascinating Mathematical People: Interviews and Memoirs

Donald J. Albers and Gerald L. Alexanderson (editors),
Princeton University Press, 2011, ISBN: 978-0-691-14829-8

This book is the third in a series, following *Mathematical People* (1985) and *More Mathematical People* (1990), of interviews and memoirs of notable mathematicians. These interviews took place between 1992 and 2005, and most were originally published in *The College Mathematics Journal*.



The subjects are mainly distinguished mathematicians such as Lars Ahlfors, Tom Apostol, Tom Banchoff, Arthur Benjamin, Dame Mary Cartwright, Richard Guy, Dusa McDuff, Donald Saari and Atle Selberg. Also included are some mathematical amateurs, like dentist Leon Bankoff, and renowned teachers and administrators such as Harold Bacon, Joe Gallian, Fern Hunt, Jean Taylor and Phillipe Tondeur. All but Benjamin were born in the first half of the twentieth century, so those not deceased are well into retirement. The book is profusely illustrated with family and conference photographs.

This is oral history at its finest! The interviewers, mainly the Editors, ask simple questions about the family, education, career, mentors, colleagues and students of their subjects, and then allow them to reminisce at will, permitting their personalities to shine through. Some are gregarious, others reserved; some are modest, others less so.

A striking feature of the collection is the diversity of backgrounds among these prominent scholars. For example, Ahlfors was born on a small Swedish-speaking island off the coast of Finland. While his father was an engineer and later a Professor of Engineering, his earlier forebears were seamen or shopkeepers on the island. Apostol, whose father was a coal miner in the small town of Helper in

Utah, was a child of Greek immigrants. Banchoff's father could have been a model for Willie Loman, the protagonist of *Death of a Salesman*. Benjamin was born to a middle-class family in Cleveland and as a child suffered from a hyperactivity disorder. Cartwright had aristocratic forebears and grew up in the period of rigid social distinctions in England before the First World War. Gallian was one who made a real wrench from his upbringing. His father worked in a glass factory in a small Pennsylvanian town and Joe followed in his footsteps in the early 1960s. The working conditions in those days were extremely hazardous, and it was only when he realised the high likelihood of losing a kneecap or worse that Joe decided he should go to college. Guy comes from a teaching background; in fact his father came to Perth in 1912 to teach at Perth Boys' School (now a National Trust heritage listed wine bar in St. Georges Terrace), joined the AIF in 1914 and took part in the Gallipoli landing. One of the most colourful interviewees is McDuff. While her father was a rather eccentric biological academic, her maternal grandfather was a Second Wrangler at Cambridge. One grandmother, who was the daughter of the Governor General of New Zealand, became the mistress and muse of H.G. Wells, who gave her the nickname Dusa, short for Medusa! Donald Saari comes from a Finnish-American farming enclave in the Upper Peninsula of Michigan. His parents were left-wing activists during the Great Depression. Selberg also came from a farming background. He was the youngest of nine children and served time in a prison camp during the Nazi occupation of Norway.

Equally diverse are their mathematical talents. Gallian and Guy are great problem setters and solvers; McDuff and Fields medallists Ahlfors and Selberg builders of vast structures; Banchoff's work in n-dimensional geometry found applications in brain research, economic models, ore geology and anthropology; Cartwright's work on nonlinear differential equations was a precursor of chaos theory; Saari has published applications in physics and astronomy as well as the social sciences.

Diversity is also evident in their range of extra-curricular interests. Bankoff was a jazz pianist, Gallian a Beatles expert. Guy and Taylor are accomplished mountaineers, Benjamin a professional conjuror. Banchoff has been consulted by ballet choreographers and the painter Salvador Dali.

Like most successful twentieth-century mathematicians, the protagonists were globetrotters and tell interesting stories of their visits. They also present vivid examples of the differences in ethos of the various institutions in which they spent their working life. We learn about Cambridge and Oxford in the 1920s, Helsinki and Zürich in the 20s and 30s, Oslo during the Second World War, Edinburgh in the 60s and of course many American private and state universities as well as the Princeton Institute for Advanced Study.

To summarise, this is a pleasant read and an ideal coffee-table book for mathematicians. There may be a case for an Australian version.

Phill Schultz
School of Mathematics and Statistics, The University of Western Australia.
Email: phill.schultz@uwa.edu.au