

# Random Curves: Journeys of a Mathematician

by Neal Koblitz

BERLIN, HEIDELBERG: SPRINGER SCIENCE +  
BUSINESS MEDIA, 2008, 392 PP., US \$34.95,  
ISBN 978-3-540-74077-3

REVIEWED BY BERNHELM BOOSS-BAVNBK

All men of any condition who have done something of special worth or something that may truly resemble those things of special merit, should, if they are truthful and good people, write in their own hand the story of their lives, but they should not begin such a fine undertaking until they have passed the age of 40.

With this verdict, the Renaissance goldsmith and sculptor Benvenuto Cellini (1500–1571) opened his own autobiography [3, p. 5], probably composed between 1558 and 1567. Neal Koblitz, the author of the autobiographical memoirs *Random Curves*, is such a Renaissance personality: A renowned top mathematician, a prolific author of widely used text books in number theory and cryptography, a harsh, polemic writer (also for 30 years for this magazine) against “mathematics as propaganda,” on elementary school mathematics teaching, and on the mathematical and general cultural life in developing countries.

No doubt, Koblitz has both “done something of special worth” in his scientific work and “something that may truly resemble those things of special merit,” though contrary to Cellini’s glorification of the bloody contemporary Florentine Medici dictatorship, Koblitz praises the rights and the virtues of the suppressed, minorities, women, children. Another title for his book could have been *Another Look at Enlightened Self-Interest*: Because that is what the book is about.

For most of its pages, *Random Curves* delivers a long and fascinating array of very sharp, personal and uncompromising comments on the great

political events of the second half of the 20th century: The Cold War, but also the quality of life in the former Soviet Union; the American aggression in Vietnam, but also the charisma of the solidarity and liberation movements; racism and civil rights movements; suppression in Africa and Latin America and counter forces; injustice, stupidity, brutality, arrogance of power—and the tactics and strength of the suppressed and how best to support them. Nothing passes without getting Koblitz’s well-argued “Another Look”, be it a deserved rap for widely accepted conditions or a positive explanation of widely rejected circumstances. He is highly opinionated and displays a total absence of the politeness associated to fashionable social constructivism and relativism.

Throughout the book, Koblitz is opinionated with good reason: He writes only of things he seems to have investigated thoroughly, and he is, more than most, aware of possible fatal consequences of careless disregard for logic and truth. There is no tolerance for superficial political thinking. Thoughtlessness is perceived by Koblitz as almost worse than bad will or selfishness, like the saying: “It is terrible to be knocked down by a car, but much more terrible to be trampled down by a hundred geese.” As in grading mathematical exercises, Koblitz vigorously discloses the slightest weakness in common arguments; and as in mathematical proofs, and contrary to common political arguing and military tactics, Koblitz always attacks his adversaries’ strongest positions. That makes reading *Random Curves* sometimes offending, often demanding, but always rewarding.

Koblitz also displays a warm and human enlightened self-interest associated with his extensive work for solidarity and charity. He doesn’t underplay the contradiction between his almost hedonistic life as a highly gifted, tenured, respected and well-paid university professor in mathematics and the miserable circumstances of the people he tries to help. *Random Curves* is not so much about his own sacrifices, renunciation, risks, punishments (though they are there), as about the emotional reward for his political activism and the wide range of possibilities an individual really has: I

did not tire of reading of his and his wife Ann Hibner’s happiness (she a math historian with a profound *Kovalevskaja* biography [7] and prolific anthropologist and gender researcher), about their travels, their organizational work, their endowments, their encounters with so many interesting, impressing and sympathetic people around the world. Koblitz is a good writer: People are described in a lively way, with a lot of humor, but always with high respect, whether he recalls the words of a schoolboy in rural Peru or of the Vietnamese Prime Minister. This human touch hopefully reconciles even a conservative reader who otherwise may feel repelled by the hard inexorable logic of Koblitz’s political arguing.

There is not much about mathematics in the book, just a few rather sketchy comments about Koblitz’s personal path into number theory at Harvard, Princeton and Moscow; then just 32 pages on his seminal work on elliptic curve cryptography (ECC) and his continuing vendetta against claims by the proponents of the mainstream public-key cryptography algorithm RSA; and, finally, 21 pages on elementary math education and math teacher education. Contrary to model autobiographies like Norbert Wiener’s *I Am a Mathematician* [9] which enthusiastically discusses control theory, prediction, Fourier analysis and brain research, or Mark Kac’s *Enigma of Chance* [6] which explores the interface between different fields of mathematics and statistical mechanics and explains, for example, the combinatorial rules of phase transition, Koblitz seems convinced by Mark Kac’s proclamation [6, p. xiii]: “The autobiography of a mathematician must contain some mathematics. Yet a presentation in popular form of some of the problems and ideas with which I have been involved throughout my life is unfortunately an impossible task.” Nevertheless, Kac tried. That was good. Koblitz did not really try. That is a pity.

Surely, Koblitz may have had good reasons for that restraint. He describes his life-long fight against overhyped ideas, often connected to improper numericity, when people dress up poor understanding or even fraudulent arguments by slick, pompous, false and misleading manipulation of logic

and numbers. Understandably, but unfortunately, he restrains himself then from giving more detailed explanations of his own work. He must have been afraid that such explanations could give the impression of adequate description while in reality and by necessity remaining superficial.

Perhaps it is not a bad choice Koblitz has made for this book, rather carefully describing the math environment instead of the mathematics itself. There, in the mathematician's everyday life, he has observed much and has much to say: On the nice and generous personality of many mathematicians, how easy it was and is from the rather remote and protected position in a math department to mix with politics even on the outspoken left, and how to make use of ties with sympathetic professionals. Strangely enough, when writing about the mathematical life, he sees everything through rose-colored spectacles and seems ready to make any compromise, even to close his eyes and shut his ears, like so many otherwise very critical mathematicians, such as Laurent Schwartz [8]. For a possible explanation, I quote Elias Canetti [2]: "Don't tell me who you are. I want to worship you."

#### Three Examples:

I. With reference to C. P. Snow, Koblitz notices the gap between different cultures, and he praises, unreservedly, a math community with values solely associated to "intellectual achievements." Snow was not so one-sided, and even less so was his source Benjamin Disraeli [4], who coined the "Two Nations" concept when he was a social critical writer, before becoming the conservative British politician and Prime Minister.

Where has Koblitz been the last 30 years? On what Mount Olympus? He doesn't seem to be aware of the breakdown of the peer referee system in mathematical journals, now that all mathematicians are pressed by their deans to publish more and shorter articles; to make a small epsilon variation into a separate note at once rather than wait for full solution; to establish friendship circles of mutual citation for higher impact factors; not to waste time as a referee for uncredited and time-consuming reading, learning and checking, an activity previously

considered highly rewarding. It seems that Koblitz doesn't know about the desperate situation of the editors of formerly highly-respected journals (names can be provided) who are deserted by their referees and, consequently, must stick to short superficial checks of submitted papers by the opinion leaders in a field. (Often, it seems, the opinion leaders do not have the time to check more than whether and how they are quoted.)

II. Even more mysterious is the author's reluctance to address the role of mathematics in the various wars fought by his country, in particular in Vietnam three decades ago, then in Kosovo (Yugoslavia) and now in Iraq and Afghanistan. Koblitz brushes aside G. H. Hardy's concerns regarding military applications of mathematics (long before the cryptography potential of number theory became evident), by one single claim regarding cryptography: "Earlier systems for scrambling messages worked well in military or diplomatic applications, where there was a fixed hierarchy of people who were authorized to know the secret keys. By the 1970s, with major sections of the economy rapidly becoming computerized, the limitations of classical cryptography were coming to the fore" (p. 297f). Koblitz elaborates that claim of the purely commercial relevance of mathematical work for public-key cryptography in a speculation about what, in Koblitz's perspective, would really upset Hardy today, namely the war in Iraq—"much more than the use of number theory in cryptography" (p. 320).

I cannot judge. I'm not an expert on the high-speed cryptography now indispensable for real-time control of military operations, and I doubt that Koblitz is. More generally, it seems to me that the mathematics historian Jens Høyrup and I have put sufficiently rich material together [1] to expect a politically attentive mathematician to make the connection between mathematics and modern war when speaking of and against war. There is ample evidence that only the superstitious belief in the math-supported pin-point accuracy of modern weaponry could create the necessary public and political support for an aggression promising to be clean and gentle with one's own

troops and civilians. Moreover, on April 9, 2003, one month into the Iraq war, the then president of Koblitz's professional organization, the American Mathematical Society, took notice, not so much of the military role of mathematics in general, as of mathematics as a key component in the preservation of US military superiority, implicitly promising the loyal assistance of his members (and asking for adequate payment): "...for a military commander to have secure communications in the field depends on fundamental advances in number theory.... Future progress in this seemingly abstract area, by us or by hostile forces, could threaten the security of all these communications." (David Eisenbud, statement to a US congressional subcommittee overseeing the funding of the US National Science Foundation [5]).

III. Another strange aspect of *Random Curves* is what may appear as a naïve perception of corporative business. Apparently, he sees only the blessings of setting the math supported turbo on modern capitalism. Once again, for Koblitz, clearly, capitalism has its bleak sides. He advocates socialist ideas and, to a surprisingly large extent, but rather convincingly, also socialist practice as he witnessed it. But he closes his eyes once again to the role of mathematics in the modern economy, for example, in the dawn of the present financial crisis. To be fair, the book was published early in 2008, a few months before the financial crisis became visible to a large population, and with it the fatal role of the math-supported belief in the security of hedge funds and investing in real estate. How come he closes his eyes to the role of mathematicians? Here we have a man, feeling responsible for his students, his product, and for the society, his customers. What customers? In recent years, financial business has most probably employed more than half of each year's "products," also from Koblitz's department. A few mathematicians were concerned about the emerging contradiction between the math-based triumph of rational pricing of options and other derivatives and the evolving impenetrability of the financial markets. Apparently, Koblitz didn't belong to them.

Perhaps Koblitz is right: Perhaps we need *not* pay attention to the

mathematical aspects of military aggression and the capitalist economy. Perhaps it suffices to protest aggression and exploitation. It seems that Koblitiz says, “Don’t mix!” I see his point, but I can’t agree.

Who will be interested in this book? Any mathematician or historian with a desire to immerse herself/himself in the vanished world of the American civil-rights movement, in solidarity movements, in national liberation movements, and in the differences and parallels between intellectual and cultural life in different nations and different segments of society will find *Random Curves* absorbing. This is not a meticulous documentation of political moves and reactions like Noam Chomsky’s writing. Koblitiz delivers mostly oral history, with its charm and its limitations. Happily, some stories sound really old and passé. This is particularly true for Koblitiz’s reported hardships in the US Civil-Rights Movement. Regarding other events, one is tempted to recall Zhou Enlai’s alleged quip to Henry Kissinger (not reported in Kissinger’s autobiography), “It is too early to say,” when asked for his assessment of the 1789 French Revolution. This may be partly true for Koblitiz’s comments on the rise and fall of socialist ideas—in spite of the fact that he has passed the ominous age of 40 required by Cellini for a balanced view.

Older liberal and left-wing mathematicians will recognize many of

Koblitiz’s recollections and will be able to compare them with their own experiences. The book might also be attractive to young readers (possibly at the advanced high-school level but more probably college age) who like to read the intelligent and sensitive eyewitness and reflections “of a student and later a scientist caught up in the tumultuous events of his generation,” as the back cover reads. This is the kind of autobiography that I read avidly when I was a teenager, and although prior knowledge of mathematics and cryptography might be helpful, it is certainly not essential for the enjoyment of Koblitiz’s moving stories.

#### REFERENCES

- [1] Bernhelm Booß-Bavnbek, Jens Høyrup, editors. *Mathematics and War*. Birkhäuser, Basel, 2003. All chapters can be downloaded for free at <http://www.springer.com/birkhauser/historyofscience/book/978-3-7643-1634-1>.
- [2] Elias Canetti. *Nachträge aus Hampstead; Aus den Aufzeichnungen 1954–1971*. Carl Hanser, Munich, 1994; *Notes from Hampstead: The Writer’s Notes: 1954–1971*. Translated from German by John Hargraves. Farrar Straus Giroux, NY, 1998.
- [3] Benvenuto Cellini. *La vita—My Life*. Translated from Italian by Julia Conaway Bondanella and Peter Bondanella, Oxford World’s Classics, Oxford University Press, Oxford, 2002.
- [4] Benjamin Disraeli. *Sybil: Or the Two Nations*. Oxford World’s Classics, Oxford University Press, Oxford, 1998.
- [5] David Eisenbud. Statement to a US Congress subcommittee overseeing the funding of the US National Science Foundation, *Notices of the AMS*, June–July 2003: 704f; <http://www.ams.org/notices/200306/inside.pdf>.
- [6] Mark Kac. *Enigmas of Chance: An Autobiography*. Sloan Foundation Series, Harper and Row, New York, 1985. Published posthumously with a memoriam note by Gian-Carlo Rota.
- [7] Ann Hibner Koblitiz. *A Convergence of Lives: Sophia Kovalevskaja, Scientist, Writer, Revolutionary*. Birkhäuser, Boston, 1983. [Reviewed in *The Mathematical Intelligencer*, 7/4:69–73, 1985.].
- [8] Laurent Schwartz. *A Mathematician Grappling with His Century*. Birkhäuser, Boston, 2001. A translation in English of Laurent Schwartz’s autobiography, *Un mathématicien aux prises avec le siècle*, originally published by éditions Odile Jacob, Paris, 1997.
- [9] Norbert Wiener. *I Am a Mathematician*. Victor Gollancz Ltd., London, 1956.

Department of Science, Systems  
and Models / IMFUFA  
Roskilde University  
DK-4000 Roskilde  
Denmark  
e-mail: booss@ruc.dk



<http://www.springer.com/978-3-540-74077-3>

Random Curves

Journeys of a Mathematician

Koblitz, N.

2008, IX, 392 p., Hardcover

ISBN: 978-3-540-74077-3