

Letters to the Editor

Shouldn't Differentiability Imply Continuity?

Regarding Niall Ryan's "The Last(?) Word in Rigor" in the June/July 2014 *Notices*: The author suggests defining derivatives by taking the limit, as positive dx goes to zero, of $[f(x+dx/2)-f(x-dx/2)]/dx$, finding this superior to the left or right derivative. This would change the definition of differentiability! While the author's proposal indeed is elegant and symmetric, it fails to detect removable discontinuities: the derivative of a function would remain unchanged if its values were altered arbitrarily on a discrete set. At least the left derivative guarantees left continuity, which I prefer to no continuity. The usual definition, allowing dx to go to zero through both positive and negative values, is the one I find most elegant and the one I like best.

—Michael Maltenfort
College Adviser and
Lecturer in Mathematics
Northwestern University
malt@northwestern.edu

(Received July 19, 2014)

The Plight of the Researcher Working Outside the University

It is sad but true that nonacademic researchers have a very difficult time in getting fair, open-minded readings of their papers. On the one hand, this is understandable, since I know from my own experience that the vast majority of papers from such researchers are crackpot works. But on the other hand, that does not mean they are all crackpot works.

Over the history of mathematics, some of the best of the best worked entirely outside the university—Descartes, Pascal, Fermat, Leibniz, and Galois, to name the most famous. In the nineteenth century, several of the leading mathematicians worked outside the university for large periods of their professional lives: Weierstrass, Dedekind, and Cayley, among others. In the twentieth century, the same was true for Chaitin and Mandelbrot, among others.

Nonacademic researchers cannot simply submit their papers directly

to journal editors, because if the work concerns a very difficult problem, the editors simply decline to consider the papers—especially if the author does not have a degree in mathematics (mine is in computer science). This has been the case with a paper of mine ("A Solution to the $3x + 1$ Problem" on <http://occampress.com>). The open-forum journals are willing to publish such papers, but publication in these journals counts for little in the academic community.

So the nonacademic researcher is forced to spend a considerable amount of his time writing letters and sending copies of his papers to individual mathematicians he selects from faculty lists on the Internet—a very inefficient and discouraging process, since mathematicians, understandably, almost invariably ignore such material.

I am wondering what readers think.

—Peter Schorer
Occam Press
peteschorer@gmail.com

(Received September 1, 2014)

Opposing an NSA Boycott

Some mathematicians are urging boycotts and other political actions based on overwrought laments about the National Security Agency (NSA). For example, in a Letter to the Editor in the December 2013 issue of the *Notices*, Alexander Beilinson suggests that "the AMS sever all ties with the NSA" because "the NSA destroyed the security of the Internet and privacy of communications for the whole planet."

There is a long history of academics getting over-excited about relatively inconsequential issues. Back in the 1970s, academics accused the NSA of crippling the Data Encryption Standard (DES) in order to spy on everyone. In fact DES was a big advance over anything else in the public domain and more secure than what IBM developed on its own. Years of analysis have not turned up any backdoors in DES, and the most practical attack is a brute-force key space search.

More recently it has been alleged that the NSA put a backdoor in a pseudo-random number generator.

Maybe so, but this possibility was publicly exposed long before Snowden, and there are no known security breaches attributable to it. In fact, the NSA has enabled improved Internet security, for example by promoting elliptic curve cryptography.

Almost every day, news stories about deliberate and accidental privacy invasions occur, and they cannot be blamed on the NSA. Google and Facebook are huge multi-billion dollar companies that make all their money by inducing you to use free services, spying on you while you do, and then selling ads based on your preferences. When your privacy is not being sold, it is being stolen. Nearly everything about you is being tracked, recorded, archived, indexed, sold, and used for commercial purposes. Most of this is unregulated. New technologies are likely to accelerate this trend.

What is more, these companies often fail to protect your private information. Consider for example the recent Heartbleed bug. The bug stemmed from a weakness in OpenSSL, which is widely used by most of the biggest Internet companies because it is free. They do not even pay the library maintainers to find and correct bugs. For a couple of years, anyone could have opened a supposedly secure connection to a Web server and scooped up a random 64K bytes of the server's secrets.

It is hard to understand why it would be acceptable for giant commercial companies to collect invasive personal information on you and to sell it to advertisers and others, but not for the NSA to check it against lists of foreign threats. Perhaps that is why there is very little public outrage over the Snowden leaks.

If you think that the NSA should jump through more hoops to access the telephone meta-data of a terrorism suspect, then go ahead and complain to your elected officials. But if personal privacy is your real concern, then the NSA is just a smokescreen. Much bigger threats are elsewhere.

Roger Schlafly
Scotts Valley, CA
roger@darkbuzz.com

(Received June 28, 2014)