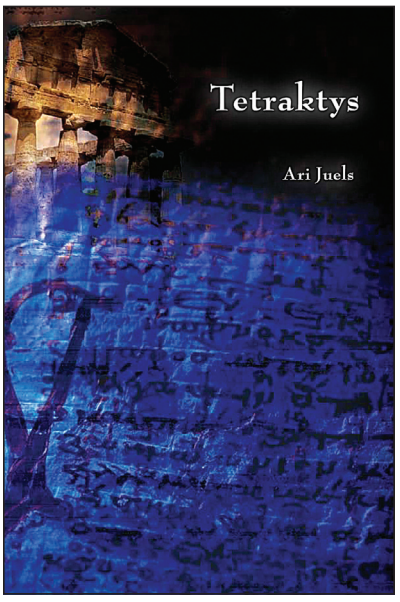
BOOK
REVIEW

MYSTICAL MATH

By Gregory Conti

Tetraktys
Ari Juels
Emerald Bay Books
ISBN-13: 978-0-9822837-0-7
$25.00



Admittedly, the idea of a computer scientist, even a top-tier one like Ari Juels, writing fiction concerned me at first. It's not that a computer scientist can't write good fiction, it's just that there can be a wide cultural, even spiritual, gap between conducting quality research and writing quality fiction that may be impossible for all but a rare voice to cross. However, *Tetraktys* elegantly creates a bridge to provide compelling and intellectually stimulating reading for the technologist and the Luddite alike.

Tetraktys is the story of Ambrose Jerusalem, a Berkeley Ph.D. student on the cusp of completing his dissertation. As both cryptographer and classicist, Ambrose is recruited by the National Security Agency to analyze a string of attacks against major corporate and governmental nodes that all lead to an unsettling conclusion: RSA encryption has been broken because the problem of efficiently factoring large numbers has been solved. Factorization is the discovery of integer divisors of numbers, such that the divisors, when multiplied, equal the original number. The RSA encryption algorithm assumes that factoring large numbers is computationally infeasible. If this assumption is incorrect, RSA fails. The clues being uncovered lead the NSA to believe that a Pythagorean cult is behind the attacks. Founded by Pythagoras, an ancient Greek philosopher and mathematician, famous for the Pythagorean Theorem attributed to him, the cult originated as a dedicated band of his most devout followers. Long considered a myth, NSA believes the cult exists today, perhaps after remaining underground for centuries, and that the Pythagoreans possess the secret of factoring efficiently and are prepared to exploit it. However, the Pythagorean ethos is so foreign that the NSA and its technologist culture is stymied. Ambrose, however, has an unusual affinity with classical culture and is brought in to help. Being told "Your country needs you" is enough to get him started.

That affinity distinguishes Ambrose from most technologists and is what makes the book so interesting. Besides being a cryptographer, Ambrose was raised and "homeschooled" by his father, a classical archeologist. As a boy he memorized Latin poetry and used Euclid as a textbook on geometry. As a result, he is an adept member of both tribes, a rare combination. He possesses connections to and understanding

of antiquity the NSA desperately lacks but at the same time deeply understands mathematics and its practical application to technology, particularly network communication and cryptography. He is an ideal translator and analyst. Computer scientists often think in terms of zeroes and ones, but it is refreshing as a reader to see the world through the eyes of a technically savvy filter like Ambrose, particularly when observing the interplay and tension among science, religion, and government.

Tetraktys reflects a hauntingly autobiographical mood. I'm sure each of us has wondered how our lives would differ if we had made alternative choices along the way. *Tetraktys* strikes me as a similar excursion. In real life, Juels is the chief scientist and director of RSA Laboratories, the research arm of a leading security company, RSA Security, but unlike his protagonist, Juels really did earn his Ph.D. from Berkeley in computer science. However, he also studied classical literature at Oxford University and Amherst College. The striking similarity between protagonist and author adds to the authenticity of the novel and makes one wonder if Ambrose Jerusalem is indeed Ari Juels and if *Tetraktys* is more memoir than fiction, albeit in a parallel world.

The most compelling aspect of the book is its intellectual stimulation and insightful technological authenticity. We are exposed to a tide of intriguing ideas with startling implications for personal privacy, technical innovation, and national security. Consider the implications of efficient factorization. Especially alarming is that one of the world's bedrock encryption algorithms would or even could fail. Current and historical communications would instantly devolve into plaintext. As an aside, we may experience these implications firsthand if quantum computers would become viable in the not-too-distant future. (Juels indicated his doubts about the state of quantum computers, saying those in an NSA office were "home-grown-looking apparatus entangled in wires, paper labels, and sheets of Mylar.") *Tetraktys* suggests many other novel ideas, most notably data mining trends in the global psyche by way of an uptick in prices on eBay or ubiquitous audio, video, and location monitoring of people via their trojaned cell phones. Another is the geolocation of users across the Internet. Traditionally, tracking an attacker back across a network involves gathering log information from each hop along the way, sometimes a legally impossible task if an intermediary is uncooperative. But Juels suggests it might be possible to use global Internet latency "conductivity maps" to triangulate the position of an attacker without such knowledge.

As a final example, Juels describes "corridors" connecting virtual worlds and the real world. People become so immersed in their virtual-world experience that they create hybrid real-world/virtual-world homes—where computer monitors cover their real-world windows and display the view from their virtual-world counterparts. As virtual-world popularity grows, it is important to consider where such corridors might lead us, particularly when the real world offers little opportunity for much of the global population compared to the potentially rich possibilities online.

No book, even this one, is perfect, of course; the complexity of a bulletproof, intricate storyline creates a challenging task for any writer. Several situations in *Tetraktys* raise questions about the consistency of the plot. For instance, why would the antagonists help total strangers win a convenience-store lottery as a public relations stunt? Moreover, why is NSA so apparently unaware of Ambrose's comings and goings? Such details are few and minor and ultimately don't undermine the plotline's plausibility and momentum.

Few people besides Juels could have written such a book, especially with such authenticity. Playing to his strengths as scientist, cryptography expert, and classically trained thinker, he delivers a tale that is compelling, intellectually stimulating, and destined to resonate with the technical community. ◀

Gregory Conti (conti@acm.org) is an assistant professor of computer science and Director of West Point's Cyber Security Research Center. He is the author of two non-fiction books: *Googling Security* and *Security Data Visualization*.

The views expressed here are those of the author and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, the Department of Defense, or the U.S. Government.

DOI: 10.1145/1655737.1655746