Inside the AMS

From the AMS Public Awareness Office

News from the 2016 Joint Mathematics Meetings (JMM): **2016 Mathematical Art Exhibition Awards.** The 2016 Mathematical Art Exhibition Awards were made at JMM "for aesthetically pleasing works that combine mathematics and art". *45 Poppies* by Karl Kattchee was awarded best photograph, painting, or print; *Sword Dancing* by George Hart was awarded best textile, sculpture, or other medium; and *OSU Triptych No. 2* by Robert Orndorff received honorable mention. See the press release for images and descriptions of these works and for information about the award at `www.ams.org/news?news_id=2929`.

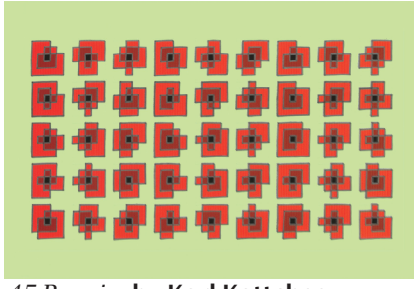

Photo Courtesy of Karl Kattchee.

45 Poppies **by Karl Kattchee**

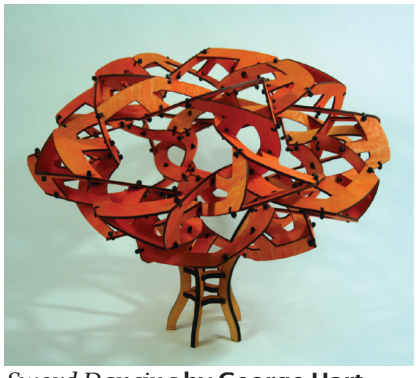

Photo Courtesy of George Hart.

Sword Dancing **by George Hart**

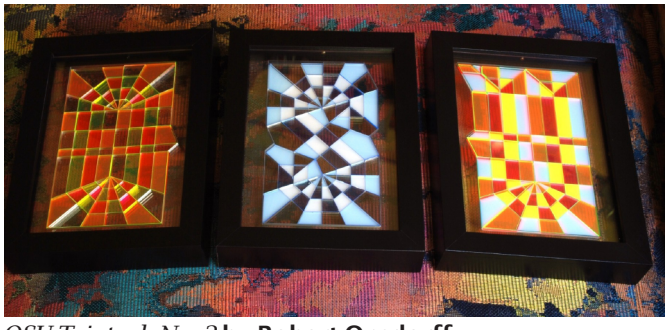

Photo Courtesy of Robert Orndorff.

OSU Triptych No. 2 **by Robert Orndorff**

National *Who Wants to Be a Mathematician*. Ankan Bhattacharya, a junior at International Academy East in Michigan, won US$10,000 in the 2016 national *Who Wants to Be a Mathematician*, astounding the audience in the finals, answering very quickly and offering wonderful explanations. Ankan will receive US$5,000 for his win, and the math department at International Academy East will receive US$5,000 as well. After the game Simon Singh, who received the 2016 JPBM Communications Award for Expository and Popular Books, gave an entertaining and informative lecture, "Fermat's Last Theorem vs. The Simpsons," which was open to the public. See videos, photos, and descriptions of the game and local media coverage at `www.ams.org/programs/students/wwtbam/jmm2016`.

Photo Courtesy of Steve Schneider, JMM.

Ken Ono, Emory University, with Ankan Bhattacharya

JMM 2016 Blog. Adriana Salerno, Evelyn Lamb, and Beth Malmskog covered sessions at and offered impressions of the Joint Mathematics Meetings on the JMM 2016 Blog. Read about the *Current Events Bulletin*, Mathematically Bent Theater, the Joint Prize Session, the AWM-AMS Noether Lecture by Karen Smith, the "origami flash fold" in the AMS exhibit, the AWM Panel Discussion on "Research Collaboration Conferences for Women: Who, What, Where, When, Why and How?" and more at `blogs.ams.org/jmm2016/`.

MathJax v2.6. MathJax v2.6 is now available and can be freely downloaded. New features include (1) Completing the CommonHTML output, a faster HTML output that can be generated on both client and server, and (2) Accessibility improvements in the form of an extension to expose MathJax's internal MathML to screen readers and making the MathJax Menu accessible. AMS is pleased to be a managing partner of MathJax. See `https://www.mathjax.org/mathjax-v2-6-now-available/`.

—Annette Emerson and Mike Breen
AMS Public Awareness Officers
`paoffice@ams.org`

AMS Holds Congressional Briefing

The American Mathematical Society's annual Congressional Briefing was given on December 9, 2015, by AMS President Elect Kenneth A. Ribet (University of California, Berkeley). In his briefing, "From right triangles to modern cryptography," Ribet recounted his experience studying the arithmetic of elliptic curves as a graduate student and then lecturing on elliptic curves in Berkeley's upper-division undergraduate course in cryptography.

Photo Courtesy of Scavone Photography.

AMS President Elect Kenneth A. Ribet

Professor Ribet explained that a great deal of contemporary cryptography depends on the apparent difficulty of computing discrete logarithms in the group of nonzero integers modulo a sufficiently large prime number. To guard against "index calculus" algorithms for computing discrete logarithms, the prime number needs to be taken so large that the calculations needed for everyday cryptography tax the batteries and processing power of small devices like smartphones.

If one replaces the group of non-zero numbers mod a prime by the group of points of an elliptic curve over a finite field, one avoids the index calculus attacks and therefore may work with smaller numbers than would be needed otherwise.

Ribet went on to say that the study of elliptic curves is ongoing and that companies like Microsoft use them in all sorts of products to provide security. The National Institute of Standards and Technology (NIST) even has a list of recommended elliptic curves. The AMS holds annual congressional briefings as a means to communicate information to policymakers. Speakers discuss the importance of mathematics research and present their work in layman's terms to Congressional staff as a way to inform members of Congress of how mathematics impacts today's important issues.

—AMS Washington Office