Math News

Vol. XXVI, No. 3 February, 2012

Fall Course Offerings

Students are invited to examine the list of course offerings available for the Fall 2012 semester and meet with advisors.

Math 236.001	MTRF	8:00- 8:50	Lance Revennaugh	DH205
Math 236.002	MTRF	11:00-11:50	Mark Hughes	DH205
Math 236.003	MTRF	2:00- 2:50	Mark Hughes	DH205
Math 237.001	MTRF	11:00-11:50	Laxman Hegde	DH325
Math 237.002	MTRF	2:00- 2:50	Robert Forsythe	DH325
Math 238.001	MTRF	11:00-11:50	Frank Barnet	DH215
*Math 340.101	T	6:00- 8:30	Karen Parks	DH202
Math 350.001	TR	12:30- 1:45	Laxman Hegde	DH215
Math 415.001	MWF	1:00- 1:50	Robert Forsythe	DH202
Math 432.001	MWF	10:00-10:50	Frank Barnet	DH215
Math 437.001	MW	3:00- 4:15	Kurtis Lemmert	DH205
Math 451.001	MWF	2:00- 2:50	Gerry Wojnar	DH202
Math 460.001	MWF	10:00-10:50	Mark Hughes	DH325
Math 491.001	TR	3:30- 4:45	Mark Hughes	DH202
Math 680.001	MWF	11:00-11:50	Lance Revennaugh	DH206

*Note: MATH 340 does not count towards a MATH major

Scholarship Information

Students are encouraged to apply for the various mathematics-related scholarships via the new STARS online program. See https://stars.frostburg.edu/stars/. The deadline this year is April 2nd.

Lighting the Way

The women from the last issue's problem can cross like this:

1. Women 1 and 2 go across (2 min.)
2. Woman 1 returns. (1 min.)
3. Women 3 and 4 go across (10 min.)
4. Woman 2 returns. (2 min.)
5. Women 1 and 2 go across. (2 min.)

The total time required is only 2 + 1 + 10 + 2 + 2 = 17 minutes, so … mission accomplished!

KME Corner

Kappa Mu Epsilon recently inducted a large cohort of new members at its annual ceremony. Welcomed to membership in the honor society were Devota Aabel, Raymond Azenadaga, Joshua Green, Joshua McDonald, DeVonte' McGee, Steven Moon, Jacob Reed, Andrew Siemann, Anna Struhar, Nicholas Torgerson, Debbie Wiles, and Justin Zimmermann. At the ceremony, Dr. Mark Hughes gave a talk entitled "Euler's Polyhedral Formula."

KME will be holding its annual Pi Day (3.14) bake sale in Dunkle Hall, and its annual Easter Candy Sale in April. Its next meeting is tentatively set for 6:00 p.m. on Wednesday, March 28th.

Online Encryption Flaw Found

(Excerpted from an article by John Markoff)

A team of European and American mathematicians and cryptographers have discovered an unexpected weakness in the encryption system widely used worldwide for online shopping, banking, e-mail and other Internet services intended to remain private and secure.

The flaw — which involves a small but measurable number of cases — has to do with the way the system generates random numbers, which are used to make it practically impossible for an attacker to unscramble digital messages. While it can affect the transactions of individual Internet users, there is nothing an individual can do about it. The operators of large Web sites will need to make changes to ensure the security of their systems, the researchers said.

The potential danger of the flaw is that even though the number of users affected by the flaw may be small, confidence in the security of Web transactions is reduced, the authors said. The system requires that a user first create and publish the product of two large prime numbers, in addition to another number, to generate a public "key." The original numbers are kept secret. To encrypt a message, a second person employs a formula that contains the public number. In practice, only someone with knowledge of the original prime numbers can decode that message.

For the system to provide security, however, it is essential that the secret prime numbers be generated randomly. The researchers discovered that in a small but significant number of cases, the random number generation system failed to work correctly.

The importance in ensuring that encryption systems do not have undetected flaws cannot be overstated. The modern world's online commerce system rests entirely on the secrecy afforded by the public key cryptographic infrastructure.

2012 Symposium Set

The 39th annual FSU Mathematics Symposium is set for Friday, April 20, 2012. Students are welcome at any of the sessions, which are scheduled for 9:00, 10:00, and 11:00, and also at the 1:00 featured address, "Using Online Resources to Promote Reasoning and Sense Making" by Patrick Vennebush.

All Boxed In

Given any set S of 9 distinct points within a unit square, show that there always exist 3 distinct points in S such that the area of the triangle formed by these 3 points is greater than or equal to 0 and less than or equal to 1/8.

Math News is published for students, faculty, staff, and administrators by the Department of Mathematics.