Department of Mathematics and Computer Science

Friday, March 21, 2014, 4:00

COLLOQUIUM TALK

Speaker: Patrick Coulton

Old Main 2231

Fun with Finite Galois Fields

Abstract:

We explore the roots of cyclotomic polynomials over various prime finite fields to show that the structure of the extension fields are not always what you might image. For example, consider the field $GF(2)$ and the polynomial

$$x^8 + x = x(x+1)(x^3+x+1)(x^3+x^2+1)$$

factored in terms of the irreducibles. If α is a root of $x^3 + x + 1$ then $\{1, \alpha, \alpha^2\}$ is a basis for the extension field as a vector space over $GF(2)$. In other words, the cubic polynomials indicate that the extension field is dimension 3 over $GF(2)$. Does $x^{32} + x$ have an irreducible factor of degree 5 that generates a basis for $GF(2^5)$ over $GF(2)$? What about $GF(p)$ for p prime. We will approach the subject from an intuitive perspective.

SNACKS IN FACULTY LOUNGE AT 3:30 PM.
EVERYONE WELCOME (EVEN IF YOU ARE UNABLE TO ATTEND THE TALK)