PACIFIC NORTHWEST NUMBER THEORY CONFERENCE
University of Washington, June 1-2 2013

TALK ABSTRACTS

Integral Points on Congruent Number Curves
Mike Bennett

We describe joint work with Dahmen, Mignotte and Siksek on an application of Hilbert modular forms to a Diophantine equation itself arising from the problem of classifying integral points on congruent number curves with bad reduction at at most two primes.

Various generalizations of Artin's conjecture for primitive roots
Adam Felix

A primitive root modulo a prime p is an integer which generates the group of non-zero residues modulo p. For primes p, we can always find a primitive root modulo p. In 1927, Artin conjectured that a density for the set of primes for which a fixed integer is a primitive root modulo p exists. Hooley showed that this is true upon the generalized Riemann hypothesis. Hooley's proof will be reviewed and various generalizations will be discussed.

Eisenstein cocycles on $GL_n(\mathbb{Q})$
Matthew Greenberg

In this talk on joint work with Pierre Charollois and Samit Dasgupta, I will discuss a construction of an Eisenstein (n-1)-cocycle on $GL_n(\mathbb{Q})$ based on Shintani's method. After indicating some of its arithmetic applications, I will describe our cocycles relation to other Eisenstein cocycles appearing in the literature.

49598666989151226098104244512918
Samuel S. Gross

Let $f(x)$ be a polynomial with non-negative integer coefficients for which $f(10)$ is a prime. A result of A. Cohn implies that if the coefficients of $f(x)$ are ≤ 9, then $f(x)$ is irreducible. In 1988, M. Filaseta showed that the bound 9 could be replaced by 10^{30}. Can we do better? We will answer this question, discuss other numbers similar to the one in the title of this talk, and explore some open problems related to our recent work.

Twists of Paramodular Vectors
Jennifer Johnson-Leung

Let F be a local field, let (π, V) be a smooth representation of $GSp(4, F)$ with trivial central character, and let χ be a quadratic character of conductor 1. Given a paramodular newform of level n, we construct a nonzero paramodular vector in the twisted representation $(\pi \otimes \chi, V)$ of paramodular level $n + 4$. We deduce a formula for the Fourier coefficients of twists of Siegel paramodular forms.

Uniform boundedness in terms of ramification

Álvaro Lozano-Robledo

Let $d \geq 1$ be fixed. Let L be a number field of degree d, and let E/L be an elliptic curve. Let $E(L)_{\text{tors}}$ be the torsion subgroup of $E(L)$. In 1996, Merel proved the uniform boundedness conjecture, i.e., there is a constant $B(d)$, which depends on d but not on the chosen field L or on the curve E/L, such that the size of $E(L)_{\text{tors}}$ is bounded by $B(d)$. Moreover, Merel gave a bound (exponential in d) for the largest prime that may be a divisor of the order of $E(L)_{\text{tors}}$. In 1996, Parent proved a bound (also exponential in d) for the largest p-power order of a torsion point that may appear in $E(L)_{\text{tors}}$. It has been conjectured, however, that there is a bound for the size of $E(L)_{\text{tors}}$ that is polynomial in d. In this talk, we will summarize what is known about $B(d)$, and we will show that there are polynomial bounds in certain cases, for instance when we restrict ourselves to elliptic curves defined over $\mathbb{Q}$ and then base-extend to L. Moreover, the bounds can also be expressed in terms of the smallest ramification index of a prime in L above p.

Elliptic Curve Discriminant Twins

Benjamin Lundell

In this talk, I will survey some ongoing joint work with Alyson Deines towards the following question: "When can two non-isomorphic elliptic curves have the same conductor and the same discriminant?" I will provide several examples of this phenomenon and briefly explain our general strategy for answering the question. Time permitting, I will explain how this question arises naturally when trying to compute optimal quotients of Shimura curves.

Curves and Fields for Efficient Cryptographic Pairings

Michael Naehrig

Bilinear maps derived from the Weil or the Tate pairing on elliptic curves over finite fields are versatile tools in cryptography. Finding the right pairing-friendly curve is crucial for practical performance. This talk introduces cryptographic pairings, shows how they are used in crypto protocols, and discusses the selection of curve and field parameters that enable secure and fast implementations of cryptographic pairings.

The sensual Apollonian circle packing

Katherine Stange

The curvatures of the circles in integral Apollonian circle packings, named for Apollonius of Perga (262-190 BC), form an infinite collection of integers whose Diophantine properties have recently seen a surge in interest. Here, we give a new description of Apollonian circle packings built upon the study of the collection of bases of $\mathbb{Z}[i]^2$, inspired by, and intimately related to, the 'sensual quadratic form' of Conway.