Abstracts for Number Theory Day

Monday December 5, 2011

On a conjecture of Terai

Florian Luca
Universidad Nacional Autónoma de México

Given positive integers m and r let A and B be such that

$$A + Bi = (m + i)^r.$$

The triple of positive integers (a, b, c) given by $a := |A|,\ b := |B|$ and $c := m^2 + 1$ satisfies $a^2 + b^2 = c^r$, and these integers are coprime when m is even. It turns out that there are only finitely many pairs of positive integers (m, r) with m even such that with the previously constructed (a, b, c) the relation $a^x + b^y = c^z$ holds with some triple of positive integers exponents $(x, y, z) \neq (2, 2, r)$, and furthermore all such pairs (m, r) as well as the corresponding triples of positive integer exponents (x, y, z) are effectively computable, although this presenter has not computed any explicit upper bound on $\max\{m, r, a, b, c, x, y, z\}$. In the talk, we will survey some known results about the more general conjecture of Terai concerning the Diophantine equation $a^x + b^y = c^z$, and we will outline some of the ideas that go into the proof of the previously mentioned result.

Sporadic sequences and modular forms

Shaun Cooper
Massey University, Albany

Just over ten years ago D. Zagier conducted an extensive computer search for integers a, b and c such that the sequence u_n defined by

$$(n+1)^2 u_{n+1} = (an^2 + an + b)u_n + cn^2 u_{n-1}, \quad u_0 = 1,\ \ u_{-1} = 0$$

produces only integer values. Only six nontrivial examples were found and it is conjectured that there are no others.

This talk is about a recent search for integral valued sequences defined by

$$(n+1)^3 u_{n+1} = (2n+1)(an^2 + an + b)u_n + n(cn^2 + d)u_{n-1}, \quad u_0 = 1,\ \ u_{-1} = 0.$$

Three nontrivial examples that were found are

$$(a, b, c, d) = (13, 4, 27, -3), \quad (6, 2, 64, -4) \quad \text{and} \quad (14, 6, -192, 12).$$

These sequences have some remarkable properties. For example, there are explicit formulas for the terms in each sequence as sums of binomial coefficients. There are some interesting divisibility properties that will be stated as conjectures. Moreover, the sequences turn out to be connected with modular forms of levels 7, 10 and 18, respectively.

These results, the experimental procedure that led to their discovery, and the reasons for doing the search will be described.

The number of ways of decomposing an integer into squarefree factors

Kevin Broughan
Waikato

Counting the number of ways $f(n)$ a positive integer n can be factored, with order not counting, has a long history in number theory. Early papers from Oppenheim (1927), Erdös (1941-43), have been followed by more recent works of Cranfield, Erdös and Pomerance (1986) and Balasubramanian and Luca (2011). Except in special cases, such as when n is squarefree, there is no "formula" for $f(n)$, thus providing interesting challenges. Evaluation requires assembling and counting all possible cases.

In this talk the study of $f(n)$ will be compared with that of $f_2(n)$, a count of the number of factorizations where each factor is squarefree. In this case, as if by magic, there are formulas for $f_2(n)$ having both a number theoretical and theoretical flavour.

Both functions can be used to determine which positive integers deserve to be called "highly factorable", giving different answers.

Unexpected p-adic numerical stability and the Robbins phenomenon

Kiran Kedlaya
UC San Diego/MIT

Just like real numbers, p-adic numbers cannot in general be represented exactly on a computer, and so are often represented in a "floating point" manner, i.e., as a power of p times an integer specified to a fixed precision (the"mantissa"). Again as for real numbers, this leads to accumulation of errors over the course of a calculation, and it is important to identify algorithms for which one has some numerical stability. Unlike for real numbers, however, stability of p-adic floating point arithmetic can sometimes arise unexpectedly for sophisticated algebraic reasons. This was originally discovered empirically by David Robbins in the case of the Dodgson (Lewis Carroll) algorithm for computing determinants, but one can formulate (and sometimes prove) a similar statement for many recurrences defined by rational functions which exhibit the so-called "Laurent phenomenon" (e.g., Somos sequences). Joint work with Joe Buhler.

Statistics for the number of points on curves over finite fields

Alina Bucur
UC San Diego

A curve is a one dimensional space cut out by polynomial equations. In particular, one can consider curves over finite fields, which means the polynomial equations should have coefficients in some finite field and that points on the curve are given by values of the variables in the finite field that satisfy the given polynomials. A basic question is how many points such a curve has, and for a family of curves one can study the distribution of this statistic. We will give concrete examples of families in which this distribution is known or predicted, and give a sense of the different kinds of mathematics that are used to study different families.

Two-variable p-adic L-functions of modular forms for non-ordinary primes

Byoung Du Kim
Victoria

We have two goals in this talk: First, by building upon the works of Katz, Hida, and others, we construct a two-variable p-adic L-function that interpolates the Rankin convolutions of an eigenform $f(z)$ and the theta series of Hecke characters of an imaginary quadratic field K when the prime p is non-ordinary for the eigenform $f(z)$. Second, by applying Pollack's theory to our two-variable p-adic L-functions, we construct a family of (single-variable) integral plus/minus p-adic L-functions of an elliptic curve for a supersingular prime.

Fermat Quartics and Serre's Challenge Curve

Victor Flynn
University of Oxford

Fermat himself determined all rational points on the curve $X^4+Y^4 = 1$, namely $(X, Y) = (0, 1), (0, -1), (1, 0), (-1, 0)$. The generalisation of this to $X^n + Y^n = 1$ has been well publicised! Instead we consider a different generalisation, to curves of the form $aX^4 + bY^4 = c$, and in particular the case $X^4 + Y^4 = c$. For many values of c one can find all rational points using elementary congruence arguments or by maps to elliptic curves. However, there remain occasional values of c, such as $c = 17,\ 82,\ \ldots,$ for which these elementary techniques are unsuccessful. Serre asked in particular how one might try to solve the case $c = 17$. We discuss various alternative lines of attack to try to deal with these exceptional values of c.