WORKSHOP SOLVABILITY OF DIOPHANTINE EQUATIONS
May 14-16, Lorentz Center, Leiden

ABSTRACTS

Attila Bérczes (University of Debrecen): *On arithmetic properties of solutions of norm form equations.*

Abstract. Let α be an algebraic number of degree n and $K := \mathbf{Q}(\alpha)$. Consider the norm form equation

$$N_{K/\mathbf{Q}}(x_0 + x_1\alpha + x_2\alpha^2 + \ldots + x_{n-1}\alpha^{n-1}) = b \quad \text{in } x_0, \ldots, x_{n-1} \in \mathbf{Z}. \qquad (1)$$

Let H denote the solution set of (1). Arranging the elements of H in an $|H| \times n$ array $\mathcal{H}$, one may ask at least two natural questions about arithmetical progressions appearing in H. The "horizontal" one: do there exist infinitely many rows of $\mathcal{H}$, which form arithmetic progressions; and the "vertical" one: do there exist arbitrary long arithmetic progressions in some column of $\mathcal{H}$?
In the near past both questions were studied thoroughly by Bazsó, Dujella, Hajdu, Pethő, Tadic, Ziegler and the speaker. In the talk the emphasis will be on explicit results obtained by the speaker and his co-authors (Pethő and Ziegler). More precisely, in the case when α is a root of the irreducible polynomial $x^n - a$ with $1 < a \leq 100$ the authors explicitly determined all solutions of the norm form equations (1) with $b = 1$ in which the coordinates $x_0, \ldots, x_{n-1}$ form an arithmetic progression. Similarly, when α is the root of the Thomas polynomial $f_a := X^3 - (a-1)X^2 - (a+2)X - 1$ ($a \in \mathbf{Z}$) we determined all solutions of the inequality

$$|N_{K/\mathbf{Q}}(x_0 + x_1\alpha + x_2\alpha^2)| \leq |2a + 1|,$$

whose coordinates from an arithmetic progression. The problems were solved using Baker's method, and combining it with local methods, the modular method and built-in Thue-solvers of PARI and MAGMA.

Imin Chen (Simon Fraser University, Burnaby): *Applications of* $\mathbf{Q}$*-curves to Diophantine equations.*

Abstract. The use of elliptic curves over $\mathbf{Q}$ and their modularity has shown itself to be a powerful tool for tackling certain types of diophantine questions.

Through work of Ellenberg and others, this technique has been extended to the use of **Q**-curves, a generalization of the notion of a modular rational elliptic curve. We discuss some further extensions of this technique with applications to solving cases of the equation $x^2 + y^{2p} = z^5$.

Pietro Corvaja (University of Udine): *Integral points on quasi-projective surfaces.*

Abstract. Let X be a projective variety, defined over a number field k, imbedded in a projective space, and let D be a hypersurface of X; we say that a rational point $x \in X(k)$ is S-integral with respect to D, where S is a finite set of valuations of k, if for no prime p outside S the reduction of x modulo p lies in D.
Recently, Zannier and myself found a new method to prove degeneracy of integral points on surfaces, with respect to sufficiently reducible hypersurfaces. We shall show several examples of applications to concrete surfaces, and show how the integrality conditions with respect to certain hypersurfaces correspond to divisibility or coprimality conditions on the coordinates.

John Cremona (University of Nottingham): *Unimodular Integer Circulants.*

Abstract. Cyclically presented groups have been studied for some time by group theorists, the main problem being to determine when they are trivial. After abelianisation this reduces to the question of whether certain families of integer circulant matrices are unimodular, and hence to the specific problem: given an integer polynomial $f(x)$, determine all values of n for which $|\mathrm{Res}(f(x), x^n - 1)| = 1$. It is this question which we will discuss from an algorithmic point of view, using algebraic and analytic methods (both classical and p-adic).

Lajos Hajdu (University of Debrecen): *Perfect powers in arithmetic progressions.*

Abstract. First we consider the equation

$$x(x+d)\cdots(x+(k-1)d) = by^n \tag{1}$$

in integers x, d, k, b, y, n where $k \geq 3$, $d > 0$, $\gcd(x, d) = 1$, where the largest prime divisor $P(b)$ of b is $\leq k$ and where n is a prime. In an earlier paper, Bennett,

Bruin, Győry and Hajdu determined all solutions to (1) with $b = 1$ and $k < 12$ (and under some further conditions also when $b > 1$). Recently, for $n = 2$ and $b = 1$ Hirata-Kohno, Laishram, Shorey and Tijdeman could extend this result as far as $k < 110$. (They obtained a similar result also for $b > 1$.) In the talk we report on some new developments in case of $n \geq 3$. Namely, in case of $n = 3$ with $P(b) < k$ and $k < 32$ Hajdu, Tengely and Tijdeman, and in case of $n > 3$ with $P(b) \leq 7$ and $12 \leq k \leq 17$ Győry, Hajdu and Pintér determined all solutions of equation (1), respectively. The main tools in the proofs are elliptic curves, modular forms, Chabauty's method and local arguments.
In the second part of the talk we consider a related problem, concerning mixed powers in arithmetic progressions. We present certain finiteness results (due to Bruin, Győry, Hajdu and Tengely), and in some cases we describe such progressions completely.

Wilfrid Ivorra (Université Paris 12, IUFM de Creteil): *Using various techniques to solve some ternary Diophantine equations of signature* $(p, p, 2)$.

Abstract. Let p be a prime integer ≥ 5. In this talk, we are interested in ternary Diophantine equations of signature $(p, p, 2)$, i.e., equations of the form $ax^p + by^p = cz^2$ with a, b, c in $\mathbf{Z}$. More precisely, we are concerned with the following problem: how to find integer solutions (x, y, z) of these equations? We will discuss how standard methods such as the modular method, the elliptic Chabauty method and linear forms in logarithms may be used to obtain integer solution for some special values of (a, b, c). In particular, we will show how the elliptic Chabauty method can be used for small values of p in order to obtain results in the case where $(a, b, c) = (1, -1, c)$ for a large class of c. In the case where $ab = 2^m\ell$ with $m \geq 0$, ℓ an odd prime number and $c = 1$, we will show how the modular method and linear forms in two logarithms can lead to "general" results. We will also investigate the limits of each of these methods.

Shanta Laishram (Tata Institute, Mumbai): *On the diophantine equation* $n(n + d) \cdots (n + (k - 1)d) = by^2$.

Abstract. In this talk, I will consider the equation

$$n(n + d) \cdots (n + (k - 1)d) = by^2 \tag{1}$$

in integers n, d, k, b with $\gcd(n, d) = 1$. Recently it has been proved that (1) with $b = 1$ is not possible when $d \leq 10^{10}$ or d has at most four prime divisors. I will give an idea of the proof and related results.

Florian Luca (UNAM, Morelia, Mexico): *Primitive Divisors for Lucas-Lehmer numbers: Applications.*

Abstract. We will remind the audience of the statement of the Primitive Divisor Theorem for Lucas-Lehmer sequences and present some new applications.

Ronald van Luijk (Simon Fraser University, Burnaby): *Cubic points on cubic curves and the Brauer-Manin obstruction on K3 surfaces.*

Abstract. It is well-known that not all varieties over $\mathbf{Q}$ satisfy the Hasse principle. The famous Selmer curve given by $3x^3 + 4y^3 + 5z^3 = 0$ in $\mathbf{P}^2$, for instance, indeed has points over every completion of $\mathbf{Q}$, but no points over $\mathbf{Q}$ itself. Though it is trivial to find points over some cubic field, it is a priori not obvious whether there are points over a cubic field that is galois. We will see that such points do exist. K3 surfaces do not satisfy the Hasse principle either, which in some cases can be explained by the so-called Brauer-Manin obstruction. It is not known whether this obstruction is the only obstruction to the existence of rational points on K3 surfaces.
We relate the two problems by sketching a proof of the following fact. If there exists a smooth curve over $\mathbf{Q}$ given by $ax^3 + by^3 + cz^3 = 0$ that is locally solvable everywhere, and that has no points over any cubic galois extension of $\mathbf{Q}$, then the algebraic part of the Brauer-Manin obstruction is not the only one for K3 surfaces. No knowledge about K3 surfaces or Brauer-Manin obstructions will be assumed as known.

Ákos Pintér (University of Debrecen): *Ternary equations, binomial Thue equations and applications.*

Abstract. In this survey talk we present some recent results concerning ternary equations and binomial Thue equations and we give several applications of these theorems to the classical diophantine problems (joint results with Bennett, Győry, Hajdu, Mignotte).

Samir Siksek (University of Warwick): *Chabauty for Symmetric Powers of Curves.*

Abstract. Let C be a curve of genus $g \geq 3$ and let $C^{(d)}$ denote its d-th symmetric power. We explain an adaptation of Chabauty which allows us in many cases to compute $C^{(d)}(\mathbf{Q})$ provided the rank of the Mordell-Weil group is at most $g - d$. We illustrate this by giving two examples of genus 3, one hyperelliptic and the other plane quartic.

Christopher Skinner (Princeton University): *Elliptic curves and Galois representations in the service of solving Diophantine equations.*

Abstract. The use of elliptic curves and modular forms to restrict and, in essence, count solutions to certain ternary Diophantine equations achieved spectacular success in the proof of Fermat's Last Theorem in the mid-1990's. The methods used to prove FLT have been refined since then and applied to other ternary equations of generalized Fermat-type (i.e., of the form $ax^p + by^q = cz^r$), sometimes in combination with other well-known Diophantine methods. This talk will survey how elliptic curves and modular forms come to be useful for ternary equations and the sort of information they provide about solutions.

Michael Stoll (International University, Bremen): *How to find the rational points on a rank 1 genus 2 curve.*

Abstract. In this talk, I will describe how one can combine ideas from Chabauty's method and the Mordell-Weil sieve to obtain an algorithm that determines the set of rational points on a curve of genus 2 with Jacobian of rank 1. The required input is a generator of the torsion-free part of the Mordell-Weil group and a rational point on the curve. If the algorithm terminates, it gives the correct result; termination is conditional on a certain conjecture.

Szabolcs Tengely (University of Debrecen): *Diophantine equations related to arithmetic progressions.*

Abstract. There are many results concerning special properties of arithmetic progressions. It is not difficult to exhibit three squares which form an arithmetic progression. Fermat stated and Euler proved that four distinct squares cannot

form an arithmetic progression. In this talk we consider the following three term progression

$$x^2, y^p, q^{2m},$$

where x, y, m are positive integers and p, q are primes > 2. We present some general statements on the structure of the solutions of the related Diophantine equation $x^2 + q^{2m} = 2y^p$ and we show how to solve completely this equation for certain values of q. At the end of the talk we will discuss some other problems related to this topic, unlike powers in arithmetic progressions and products of terms of arithmetic progressions.

Gary Walsh (University of Ottawa): *Integer points on various models of elliptic curves.*

Abstract. The automated determination of the set of integer points on an elliptic curve has all but been fully integrated within a number of mathmematical software packages, including MAGMA. However, difficulties arise if one attempts to solve such a problem when the subroutines incorporated within the algorithm do not have finite running time. Using recent advances in several areas of Diophantine analysis, we describe a number of families of elliptic curves, in various forms, and describe briefly how one can determine an absolute bound for the number of integer points, and in some cases, describe the set of integer points explicitly.