# Diophantine approximation and analytic number theory : a tribute to Cam Stewart
# May 30th–June 4th, 2010

## MEALS

*Breakfast (Buffet): 7:00–9:30 am, Sally Borden Building, Monday–Friday
*Lunch (Buffet): 11:30 am–1:30 pm, Sally Borden Building, Monday–Friday
*Dinner (Buffet): 5:30–7:30 pm, Sally Borden Building, Sunday–Thursday
Coffee Breaks: As per daily schedule, 2nd floor lounge, Corbett Hall
***Please remember to scan your meal card at the host/hostess station in the dining room for each meal.**

## MEETING ROOMS

**All lectures will be held in Max Bell 159 (Max Bell Building accessible by walkway on 2nd floor of Corbett Hall). LCD projector, overhead projectors and blackboards are available for presentations.** Note that the meeting space designated for BIRS is the lower level of Max Bell, Rooms 155–159. Please respect that all other space has been contracted to other Banff Centre guests, including any Food and Beverage in those areas.

## SCHEDULE

### Sunday

| | |
|---|---|
| **16:00** | Check-in begins (Front Desk - Professional Development Centre - open 24 hours) |
| **17:30–19:30** | Buffet Dinner, Sally Borden Building |
| **20:00** | Informal gathering in 2nd floor lounge, Corbett Hall |
| | Beverages and a small assortment of snacks are available on a cash honor system. |

### Monday

| | |
|---|---|
| **7:00–8:45** | Breakfast |
| **8:45–9:00** | Introduction and Welcome by BIRS Station Manager, Max Bell 159 |
| **9:00–9:30** | Lecture : Pomerance |
| **9:45–10:15** | Lecture : Vaaler |
| **10:30–11:00** | Coffee Break, 2nd floor lounge, Corbett Hall |
| **11:00–11:30** | Lecture : Luca |
| **11:30–13:00** | Lunch |
| **13:00–14:00** | Guided Tour of The Banff Centre; meet in the 2nd floor lounge, Corbett Hall |
| **14:00–14:15** | Group Photo; meet on the front steps of Corbett Hall |
| **14:30–15:00** | Lecture : Stange |
| **15:10–15:30** | Coffee Break, 2nd floor lounge, Corbett Hall |
| **15:30–16:00** | Lecture : Bugeaud |
| **16:15–16:45** | Lecture : Győry |
| **17:00–17:30** | Lecture : Shparlinski |
| **17:30–19:30** | Dinner |

**Tuesday**

| | |
|---|---|
| **7:00–9:00** | Breakfast |
| **9:00–9:30** | Lecture : Schmidt |
| **9:45–10:15** | Lecture : Velani |
| **10:30–11:00** | Coffee Break, 2nd floor lounge, Corbett Hall |
| **11:00–11:30** | Lecture : Pollington |
| **11:30–13:30** | Lunch |
| **14:30–15:00** | Lecture : Williams |
| **15:10–15:30** | Coffee Break, 2nd floor lounge, Corbett Hall |
| **15:30–16:00** | Lecture : Friedlander |
| **16:15–16:45** | Lecture : Gyarmati |
| **17:00–17:30** | Lecture : Tijdeman |
| **17:30–19:30** | Dinner |

**Wednesday**

| | |
|---|---|
| **7:00–9:00** | Breakfast |
| **9:00–9:30** | Lecture : Roy |
| **9:45–10:15** | Lecture : Sárkőzy |
| **10:30–11:00** | Coffee Break, 2nd floor lounge, Corbett Hall |
| **11:00–11:30** | Lecture : Schinzel |
| **11:30–13:30** | Lunch |
| | Free Afternoon |
| **17:30–19:30** | Dinner |

**Thursday**

| | |
|---|---|
| **7:00–9:00** | Breakfast |
| **9:00–9:30** | Lecture : Beukers |
| **9:45–10:15** | Lecture : Evertse |
| **10:30–11:00** | Coffee Break, 2nd floor lounge, Corbett Hall |
| **11:00–11:30** | Lecture : Hirata-Kohno |
| **11:30–13:30** | Lunch |
| **14:30–15:00** | Lecture : Filaseta |
| **15:10–15:30** | Coffee Break, 2nd floor lounge, Corbett Hall |
| **15:30–16:00** | Lecture : Pintér |
| **16:15–16:45** | Lecture : Baker |
| **17:00–17:30** | Lecture : Maier |
| **17:30–19:30** | Dinner |

**Friday**

| | |
|---|---|
| **7:00–9:00** | Breakfast |
| **9:00–9:30** | Lecture : Chahal |
| **9:45–10:15** | Lecture : Top |
| **10:30–11:00** | Coffee Break, 2nd floor lounge, Corbett Hall |
| **11:00–11:30** | Lecture |
| **11:30–13:30** | Lunch |

**Checkout by 12 noon.**

** 5-day workshops are welcome to use BIRS facilities (2nd Floor Lounge, Max Bell Meeting Rooms, Reading Room) until 3 pm on Friday, although participants are still required to checkout of the guest rooms by 12 noon. **

# Diophantine approximation and analytic number theory : a tribute to Cam Stewart
# May 30th–June 4th, 2010

## ABSTRACTS
### (in alphabetic order by speaker surname)

Speaker: **Roger Baker** (Provo)
Title: *Primes in arithmetic progressions to sparse moduli*
Abstract: In this class of problems, one seeks to prove an average result along the lines of the Bombieri-Vinogradov theorem, but with averaging over a sparse set of moduli, such as the values of a polynomial. Generally one has to reduce the exponent 1/2 that occurs in that theorem, but it is not clear what are.the sharpest results attainable with our existing knowledge of Dirichlet polynomials and mean values of L-functions. I give some examples, including an improvement of the result of Mikawa and Peneva, and that of Baier and Zhao, in the polynomial case.

Speaker: **Frits Beukers** (Utrecht)
Title: *Recurrent sequences coming from Shimura curves*
Abstract: In his irrationality proof of $\zeta(2)$ and $\zeta(3)$, Apéry uses some recurrence sequences which, miraculously, have integer sequences as solutions. Using Shimura curves it is possible to find similar but completely unrelated recurrent sequences. This is based on an idea of Chudnovsky and a major step in this direction has been taken in the recent PhD-thesis by Jeroen Sijsling. The curves are modular curves connected with quaternion subgroups. Unfortunately no new irrationality proofs seem to follow.

Speaker: **Yann Bugeaud** (Strasbourg)
Title: *The irrationality exponent of the Thue–Morse–Mahler number is equal to* 2
Abstract: Let $(t_k)_{k\geq 0}$ be the Thue-Morse sequence on $\{0,1\}$ defined by $t_0 = 0, t_{2k} = t_k$ and $t_{2k+1} = 1 - t_k$ for $k \geq 0$. Let $b \geq 2$ be an integer. We establish that the irrationality exponent of the Thue-Morse-Mahler number $\sum_{k\geq 0} t_k b^{-k}$ is equal to 2.

Speaker: **Jasbir Chahal** (Provo)
Title: *To be announced*

Speaker: **Jan-Hendrik Evertse** (Leiden)
Title: *On monogenic orders*
Abstract: An order in an algebraic number field $K$ is a ring $O \subset K$ which is contained in the ring of integers of $K$ and which spans $K$ as a $\mathbb{Q}$-vector space. An order $O$ generated by one element, i.e., of the shape $\mathbb{Z}[\alpha]$, is called *monogenic*. If $O = \mathbb{Z}[\alpha]$ and $\beta$ is equivalent to $\alpha$, i.e., $\beta = \pm\alpha + a$ for some $a \in \mathbb{Z}$, then $\beta$ is said to be equivalent to $\alpha$. Győry proved in an effective way, that for any given order $O$, there are only finitely many equivalence classes of $\alpha \in O$ such that $O = \mathbb{Z}[\alpha]$. An order $O$ is said to be (at most/at least/precisely) $k$ times monogenic, if there are (at most/at least/precisely) $k$ equivalence classes of $\alpha \in O$ such that $O = \mathbb{Z}[\alpha]$. The main subject of the talk is the following theorem:

**Theorem.** *Let $K$ be a number field of degree $\geq 3$. Then there are only finitely many orders $O$ in $K$ that are at least three times monogenic. If $K$ is not a CM-field, there are infinitely many orders $O$ in $K$ that are two times monogenic.*

The proof depends on a joint theorem of Győry, Stewart, Tijdeman and the speaker on unit equations in two variables. We will also give more precise information on the structure of orders that are two times monogenic.

This is partly joint work with Kálmán Győry.

Speaker: **Michael Filaseta** (Columbia) Title: *A survey of results related to the Galois structure of Laguerre polynomials*

Abstract: The Galois structure of the generalized Laguerre polynomials $L_n^{(\alpha)}(x)$ of degree $n$ was investigated by Schur in the early 1930's. For each $n$, he gave an example of an $\alpha$ for which the Galois group of $L_n^{(\alpha)}(x)$ over $\mathbb{Q}$ is the symmetric group $S_n$. He also obtained an analogous example in the case of the alternating group $A_n$ except for even $n$ not divisible by 4. Recent work in Diophantine approximation of independent interest has led both to examples of such $\alpha$ for even $n$ not divisible by 4, in the case of $A_n$, and a proof that the examples provided are, for the most part, the only such examples. We will give a historical overview of these results, elaborating on the Diophantine preliminaries that helped lead to the above conclusions.

Speaker: **John Friedlander** (Toronto)

Title: *Semilinear Sieve, Quadratic Questions, Linnik's Legacy*

Abstract: We discuss some applications of the first item, to the second item in general, and to the third item in particular. Joint work with Henryk Iwaniec.

Speaker: **Katalin Gyarmati** (Budapest)

Title: *On pseudorandom binary lattices*

Abstract: Hubert, Mauduit and Sárkőzy introduced pseudorandom measures for pseudorandomness of binary lattices, and they gave constructions for binary lattices with strong pseudorandom properties. They gave nearly optimal upper bounds for the pseudorandom measures of the lattices constructed. However, these early constructions also have disadvantages: they are rather artificial, and their implementation is complicated. Thus another construction is presented here which is based on the use of the Legendre symbol. This construction is much more natural and flexible than the earlier ones, and it can be implemented more easily. However, there is a price paid for this: to give upper bounds for the pseudorandom measures one needs the flexibility and generality of Weil's theorem, and here in the two dimensional situation this approach leads to weaker bounds than the optimal ones.

Speaker: **Kálmán Győry** (Debrecen)

Title: *On certain arithmetic graphs and their applications*

Abstract: For an integral domain $R$ finitely generated over $\mathbb{Z}$ , denote by $G(R)$ the graph which has vertex set $R$, and whose edges are the pairs $[a, b]$ ( $a, b$ elements of $R$ ) for which $a - b$ is in $R*$ .These graphs , in certain special cases, were introduced by the speaker in the 1970's, and in general in the 1980's. It turned out that many diophantine problems can be reduced to the study of connectedness properties of finite induced subgraphs of such graphs $G(R)$. These induced subgraphs have been characterized in terms of connectedness which led to several important applications. The first part of the talk will be devoted to a brief historical overview. In the second part some new quantitative diophantine results will be presented on the finite induced subgraphs of $G(R)$. Some applications will also be formulated for polynomials with given discriminant, for simple integral ring extensions, for pairs of polynomials with given resultant and for irreducible polynomials of the form $g(f(x))$. This latter application is joint work with L.Hajdu and R.Tijdeman. Finally, some new effective results of J.H.Evertse and the speaker will be mentioned on polynomials and integral elements of given discriminant.

Speaker: **Noriko Hirata-Kohno** (Tokyo)

Title: *Iwasawa p-adic logarithmic function and applications*

Abstract: We review the role of Iwasawa $p$-adic logarithmic functions in the theory of transcendence. We then discuss how we manage to extend the domain of the definition of $p$-adic elliptic logarithmic functions and show applications in the estimate of linear forms in logarithms.

Speaker: **Florian Luca** (Morelia)
Title: *On an interesting property of* 2671546041964800
Abstract: Let $f(n)$ be the function which associates to $n$ the number of ordered factorizations of $n$ in prime parts. If

$$n = p_1^{r_1} \cdots p_k^{r_k}$$

then

$$f(n) = \binom{r_1 + \cdots + r_k}{r_1, r_2, \ldots, r_k}.$$

Call $n$ to be *prime-perfect* if $f(n) = n$. For example, the number given in the title whose factorization is

$$2^8 \times 3^6 \times 5^2 \times 7^2 \times 11^2 \times 13 \times 17 \times 19 \times 23$$

is prime-perfect. We have four more examples of prime-perfect numbers. In my talk, I will show that there are only finitely many $n$ with such property and in fact the largest one satisfies $n < 10^{10^{100}}$.
This is joint work with Arnold Knopfmacher from Wits University in Johannesburg, South Africa.

Speaker: **Helmut Maier** (Ulm)
Title: *The behaviour in short intervals of exponential sums over sifted integers*
Abstract: We give a conjecture on the behaviour in short intervals on exponential sums over prime numbers and show that this conjecture will imply the twin prime conjecture. We then show that an analogous conjecture is satisfied, if the set of prime numbers is replaced by a certain set of integers without small prime factors.

This is joint work with A. Sankaranarayanan.

Speaker: **Ákos Pintér** (Debrecen)
Title: *Diophantine equations and modular forms*
Abstract: In this talk we report on some applications of modular technique to classical diophantine problems including the power values of power sums, resolution of binomial Thue-equations and perfect powers from products of consecutive terms in arithmetic progression. These results are joint works with Bennett, Győry, Hajdu and Mignotte.

Speaker: **Andy Pollington** (NSF)
Title: *Finite collections of the sets $Bad(i,j)$ have non-empty intersection: solution to a question of Wolfgang Schmidt*
Abstract: If $i \geq 0$ and $j = 1 - i$ we say that $(\alpha, \beta) \in Bad(i,j)$ if there is a constant $c > 0$ such for for every natural number $q$

$$\max(\|q\alpha\|^{1/i}, \|q\beta\|^{1/j}) > c/q.$$

Any counter example to Littlewood's conjecture in Diophantine approximation must belong to every $Bad(i,j)$ set.

If these sets had empty intersection then Littlewood's conjecture would follow. Schmidt asked if it is true that the sets $Bad(1/3, 2/3)$ and $Bad(2/3, 1/3)$ have non-empty intersection. We prove this and show that the sets involved have full dimension. This is joint work with Dzmitry Badziahin and Sanju Velani.

Speaker: **Carl Pomerance** (Dartmouth)
Title: *Fibonacci Integers*
Abstract: A Fibonacci integer is an integer in the multiplicative group generated by the Fibonacci numbers. For example, $77 = (21 \times 55)/(3 \times 5)$ is a Fibonacci integer. Up to 100 there are 88 of them, so they appear to be fairly common. But are they really? Using some results about the structure of this group, we obtain a near-asymptotic formula for the counting function of the Fibonacci integers. Our proof is based on both combinatorial and analytic ideas. (Joint work with Florian Luca and Stephan Wagner.)

Speaker: **Damien Roy** (Ottawa)
Title: *Recent progress on Diophantine approximation in small degree*
Abstract: Starting with the pioneer work of Davenport and Schmidt in 1969, we present some recent results concerning the problem of simultaneous approximation to few numbers by rational numbers with the same denominator, and related questions of approximation to real numbers by algebraic numbers of restricted types, as well as versions of Gel'fond's criterion. This includes work of Adamczewski, Bel, Bugeaud, Laurent, Lozier, Teulié, Zelo ... and a partial answer to a question of Cam Stewart. Happy birthday Cam!

Speaker: **Andras Sárkőzy**
Title: *On arithmetic properties of sums $a + b$ and shifted products $ab + 1$*
Abstract: The study of arithmetic properties (prime factors, number of prime factors, square factors, etc.) of sums $a + b$, resp. shifted products $ab + 1$ with $a, b$ belonging to given "large" or "dense" sets $A, B$ of positive integers is a classical field. The first problem of this type involving shifted products was studied by Diophantus, the first result on prime factors of sums $a + a'$ was proved by Erdos and Turan. In my talk I will focus on our joint work with Cam Stewart in this field. Two typical results: we proved that if A, B contain more than $cn$ positive integers up to $N$ then there is a sum a+b whose greatest prime factor is $c'N$ (and we proved a similar result on prime powers in place of prime factors); moreover, Győry, Cam and I showed that if $A, B$ are large sets of positive integers then the product of the shifted products $ab+1$ has "many" distinct prime factors.

Speaker: **Andrzej Schinzel** (Warsaw)
Title: *Multiplicative properties of sets of integers*
Abstract: It is proved that for more than 99% of all moduli $m$,if a set of residues mod $m$ has at least $m/2$ elements,then it contains residues $r_1, r_2, r_3$ such that $r_1 r_2 = r_3$.

Speaker: **Wolfgang Schmidt** (Boulder)
Title: *To be announced*

Speaker: **Igor Shparlisnki** (Sydney) Title: *Fermat quotients*
Abstract: We show that for a prime $p$ the smallest $a$ with $a^{p-1} \not\equiv 1 \pmod{p^2}$ does not exceed $(\log p)^{463/252+o(1)}$ which improves the previous bound $O((\log p)^2)$ obtained by H. W. Lenstra in 1979. We also show that for almost all primes $p$ the bound can be improved as $(\log p)^{5/3+o(1)}$.

These results are based on a combination of various techniques including the distribution of smooth numbers, distribution of elements of multiplicative subgroups of residue rings, bound of Heilbronn exponential sums and a large sieve inequality with square moduli.

This is joint work with J. Bourgain, K. Ford and S. Konyagin.

Speaker: **Kate Stange** (Vancouver)
Title: *Amicable pairs and aliquot cycles for elliptic curves*
Abstract: An amicable pair for an elliptic curve $E/\mathbb{Q}$ is a pair of primes $(p, q)$ of good reduction for E satisfying $\#E(F_p) = q$ and $\#E(F_q) = p$. Aliquot cycles are analogously defined longer cycles. Although rare for non-CM curves, amicable pairs are – surprisingly – relatively abundant in the CM case. We present heuristics and conjectures for the frequency of amicable pairs and aliquot cycles, and some results for the CM case (including the especially intricate $j = 0$ case). This is joint work with Joseph H. Silverman.

Speaker: **Rob Tijdeman** (Leiden)
Title: *Applications of linear forms estimates by Cam Stewart*

Speaker: **Jaap Top** (Groningen)
Title: *Discriminant surfaces*

Abstract: In this talk we will discuss classical geometric properties of the discriminant of a polynomial. Most results on this date from the 19th century. The fascinating history of the topic provides a story which I hope you will enjoy as much as I do!

Speaker: **Jeff Vaaler** (Austin)
Title: *Heights on finitely generated groups and a multiplicative form of Siegel's lemma*
Abstract: Let $\mathcal{A}$ be a finitely generated subgroup of $\overline{\mathbb{Q}}^*$. We define an absolute height $h(\mathcal{A})$ that generalizes the absolute logarithmic Weil height on subgroups of rank 1. By applying methods from a recent joint paper with D. Allcock, we prove that if $\mathcal{A}$ has rank $N$, then there exist $N$ multiplicatively independent elements $\alpha_1, \alpha_2, \ldots, \alpha_N$ in $\mathcal{A}$ such that

$$h(\alpha_1)h(\alpha_2)\cdots h(\alpha_N) \le h(\mathcal{A}),$$

and the subgroup generated by $\alpha_1, \alpha_2, \ldots, \alpha_N$ has index at most $N!$ in $\mathcal{A}$. The proof uses the fact that the completion of $\overline{\mathbb{Q}}^*/\mathrm{Tor}(\overline{\mathbb{Q}}^*)$ with respect to the metric induced by the absolute Weil height is a real Banach space, and so its $N$-dimensional subspaces are isomorphic to $\mathbb{R}^N$.

Speaker: **Sanju Velani** (York)
Title *Badly approximable sets within the context of the Schmidt and Littlewood conjectures*

Speaker: **Hugh Williams** (Calgary/Ottawa)
Title: *A Problem Concerning Divisibility Sequences*
Abstract: A sequence of rational integers $\{A_n\}$ is said to be a divisibility sequence if $A_m \mid A_n$ whenever $m \mid n$. If the divisibility sequence $\{A_n\}$ also satisfies a linear recurrence relation, it is said to be a linear divisibility sequence. The best known example of a linear divisibility sequence is the Lucas sequence $\{u_n(p,q)\}$, one particular instance of which is the famous Fibonacci sequence. One way to generalize the Lucas sequence is to consider linear divisibility sequences which have a characteristic polynomial of even degree $2k$, and distinct zeros with the property that $k$ pairs of these zeros have the same integral product. The case of $k = 1$ is, of course, the Lucas sequence. In this talk I will discuss the case of $k = 2$. This deceptively simple sounding investigation turns up some rather difficult problems.