SCHEDULED TALKS AND THEIR ABSTRACTS FOR "DIOPHANTINE ANALYSIS AND RELATED FIELDS 2012"

Takao Komatsu (Hirosaki Univ.)

Title: *Poly-Cauchy numbers and Riordan arrays*

Abstract: Poly-Cauchy numbers $c_n^{(k)}$ are defined by

$$c_n^{(k)} = \underbrace{\int_0^1 \cdots \int_0^1}_{k} (x_1 x_2 \cdots x_k)(x_1 x_2 \cdots x_k - 1) \cdots (x_1 x_2 \cdots x_k - n + 1) dx_1 dx_2 \cdots dx_k \,.$$

If $k = 1$, then $c_n^{(1)} = c_n$ are the classical Cauchy numbers. Poly-Cauchy numbers have some similar properties as poly-Bernoulli numbers which are introduced by M. Kaneko and are some kinds of generalization of the classical Bernoulli numbers. In this talk we give some characteristic properties and relations with Riordan arrays.

Takao Komatsu and Mari Yokohama (Hirosaki Univ.)

Title: *A generalization of poly-Cauchy numbers*

Abstract: In this talk we give a generalization of poly-Cauchy numbers. Namely, we define the poly-Cauchy numbers with q parameter $c_{n,q}^{(k)}$ by

$$c_{n,q}^{(k)} = \underbrace{\int_0^1 \cdots \int_0^1}_{k} (x_1 x_2 \cdots x_k)(x_1 x_2 \cdots x_k - q) \cdots (x_1 x_2 \cdots x_k - (n-1)q) dx_1 dx_2 \cdots dx_k \,.$$

Poly-Cauchy numbers with q parameter also have explicit formulae by using Stirling numbers of the first kind, and have the corresponding generating functions.

Noriko Hirata-Kohno (Nihon Univ.)

Title: *Arithmetic properties of p-adic elliptic polylogarithmic functions*

Abstract: In the talk, we investigate arithmetic properties of p-adic elliptic polylogarithmic functions by using a formal group. Let $t \in \mathbb{C}_p$ with $|t|_p < 1$. We define the p-adic k-th polylogarithmic function by $Li_{\mathcal{E},1}(t) = \log_{\mathcal{E}}(t)$ and $Li_{\mathcal{E},k}(t) = \int_0^t \frac{Li_{\mathcal{E},k-1}(u)}{u} du$ $(k = 2, 3, \cdots)$. We give bounds for the height of the Taylor coefficients of our p-adic elliptic polylogarithmic functions and show several new arithmetic properties.

Yuri V. Nesterenko (Moscow State Univ.)

Title: *Some identities of Ramanujan type*

Abstract: We will discuss identities of modular type that are proved for some functions $g_{u,v}(\tau)$ that looks like Eisenstein series. They generalize some classical identities of S. Ramanujan and E. Grosswald. At the point i these identities give linear relations over $\mathbb{Q}$ connecting ζ-values at odd points and values $g_{u,v}(i)$. As a consequence we proved that the transcendence degree of the field generated by the values of $g_{u,v}(\tau)$ is smaller that it is expected.

Hajime KANEKO (Nihon Univ.)

Title: *Algebraic independence of the special values of power series and those derivatives*
Abstract: Liouville proved the transcendence of the values of $\sum_{n=0}^{\infty} b^{-n!}$, where b is an integer greater than 1. In our talk we consider algebraic independence of the values of power series at certain rational points. In particular, we give new criteria for algebraic independence of such numbers. Applying our criteria, we deduce algebraic independence of the values of power series and those derivatives at certain rational points.

Koichiro AKIYAMA (Toshiba Corp.)

Title: *Public key cryptosystem based on the diophantine problems on $F_p[t]$*
Abstract: We construct a new type of public-key cryptosystem whose security is based on the Diophantine Problems on $F_p[t]$. Public-key cryptosystems requires two keys called public key and private key. Public key is used for encrypt plaintext, and private key is used for decrypt the ciphertext. Security of public key cryptosystem relies on the problem which is difficult to solve, such as integer factorization. We employ the Diophantine Problems on $F_p[t]$ called the section finding problem (SFP) to construct public key cryptosystem. In this talk, I describe the encrypt/decrypt algorithms and key generation algorithm, and discuss about the difficulty of SFP.

Yu YASUFUKU (Nihon Univ.)

Title: *Finiteness integers in orbits of maps on $\mathbb{P}^n$*
Abstract: Silverman has proved finiteness of integers in the orbit $\{P, \phi(P), \phi(\phi(P)), \ldots\}$ of a rational point P under a non-totally-ramified morphism ϕ on $\mathbb{P}^1$. In this talk, we will discuss several generalizations of this to maps on $\mathbb{P}^n$. Some specific low-degree and low-dimensional maps are treated, using ingredients such as Schmidt's subspace theorem. We also present a theoretical result treating more general morphisms, albeit assuming a powerful conjecture in Diophantine geometry by Vojta. The hypothesis required on the morphisms has been weakened from a prior paper, so we will highlight the difference.

Takehiro HASEGAWA (Kogakuin Univ.)

Title: *A polynomial with Franel numbers as coefficients and its application to modular curves*
Abstract: In 1884 (19th century), Franel defined the number $a_n = \sum_{k=0}^{n} \binom{n}{k}^3$ and he showed that it satisfies the recurrence $(n+1)^2 a_{n+1} - (7n^2 + 7n + 2)a_n - 8n^2 a_{n-1} = 0$. In 2009, Maier gave two kinds of functional equations for the generating function $F(z) = \sum_{n \geq 0} a_n z^n$. In this talk, we obtain two polynomial identities over finite fields from these equations, and by using these identities, we explicitly describe behaviors of supersingular points in the towers $\{X_0(3 \cdot 2^n)\}$ and $\{X_0(2 \cdot 3^n)\}$.

Takeshi KUROSAWA (Tokyo Univ. Sci.)

Title: *Algebraic dependence of infinite products related with Fibonacci and Lucas numbers*
Abstract: Let d be an integer greater than 1. In [1], we gave necessary and sufficient conditions for the infinite products

$$\prod_{\substack{k=1 \\ U_{d^k} \neq -a_i}}^{\infty} \left(1 + \frac{a_i}{U_{d^k}}\right) \quad (i = 1, \ldots, m) \qquad \text{or} \qquad \prod_{\substack{k=1 \\ V_{d^k} \neq -a_i}}^{\infty} \left(1 + \frac{a_i}{V_{d^k}}\right) \quad (i = 1, \ldots, m)$$

to be algebraically dependent, where $a_1, \dots, a_m$ are nonzero integers and $\{U_n\}_{n\geq 0}$ and $\{V_n\}_{n\geq 0}$ are generalized Fibonacci numbers and Lucas numbers, respectively. In this talk, we relax the condition $a_1, \dots, a_m$ nonzero integers to real algebraic numbers. By generalizing the condition we show new algebraically dependent cases.

References

[1] T. Kurosawa, Y. Tachiya and T. Tanaka, *Algebraic independence of infinite products generated by Fibonacci numbers*, Tsukuba Journal of Mathematics **34** (2010), no. 2, 255–264.

Yohei TACHIYA (Hirosaki Univ.)

Title: *Algebraic independence of infinite products generated by distinct binary recurrences*

Abstract: Let α and β be real algebraic numbers with $|\alpha| > 1$ and $\alpha\beta = -1$. Define

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad V_n = \alpha^n + \beta^n \quad (n \geq 0).$$

If $a = (1+\sqrt{5})/2$, we have $U_n = F_n$ and $V_n = L_n$ $(n \geq 0)$, where the sequences $\{F_n\}_{n\geq 0}$ and $\{L_n\}_{n\geq 0}$ are Fibonacci and Lucas numbers, respectively.

Let $d_1, d_2 \geq 2$ be integers and γ_1, γ_2 be real algebraic numbers. The purpose of this talk is to discuss the algebraic independence over $\mathbb{Q}$ of the infinite products

$$\prod_{\substack{k=1 \\ U_{d_1^k} \neq -\gamma_1}}^{\infty} \left(1 + \frac{\gamma_1}{U_{d_1^k}}\right) \qquad \text{and} \qquad \prod_{\substack{k=1 \\ V_{d_2^k} \neq -\gamma_2}}^{\infty} \left(1 + \frac{\gamma_2}{V_{d_2^k}}\right).$$

As an application, we show that the infinite products $\prod_{k=1}^{\infty}(1+1/F_{2^k})$ and $\prod_{k=1}^{\infty}(1+1/L_{2^k})$ are algebraically independent over $\mathbb{Q}$.

Florian LUCA (Inst. de Mat., UNAM)

Title: *Balancing with powers of Fibonacci numbers*

Abstract: Let $(F_n)_{n\geq 0}$ be the Fibonacci sequence. In my talk, I will show that the only solution of the Diophantine equation

$$F_1^k + F_2^k + \cdots + F_{n-1}^k = F_{n+1}^\ell + \cdots + F_{n+r}^\ell$$

in positive integers (k, ℓ, n, r) is $(8, 2, 4, 3)$. This confirms a conjecture of Behera, Liptai, Panda and Szalay. This is joint work with A. Dujella (Zagreb) and S. Díaz Alvarado (Toluca).

Attila PETHŐ and Michael E. POHST (Univ. Debrecen)

Title: *On the indices of multiquadratic number fields*

Abstract: We present explicit formulae for the index forms of multiquadratic number fields. For octic fields we calculate all potential field indices and characterize the corresponding fields. We also show that any prime power p^k divides the field index if the degree 2^r is sufficiently large. Our method differs from all others which have been previously used.

Isao WAKABAYASHI (Tokyo)

Title: *Number of solutions for quartic simple Thue equations*

Abstract: Put $F(X,Y) = bX^4 - aX^3Y - 6bX^2Y^2 + aXY^3 + bY^4$ with integer coefficients. We show that the number of solutions for the Thue equation $F(x,y) = 1, -1$ is 0 or 4, except for a few already known cases. To obtain an upper bound for the size of solutions, we use Padé approximation method. To obtain a lower bound for the size of solutions, we construct a continued fraction with positive or negative rational partial quotients. This construction is carried out carefully by using special properties of the form F. Combining these lower and upper bounds, we obtain the result.

Yasutsugu Fujita (Nihon Univ.) and Nobuhiro Terai (Ashikaga Inst. Tech.)

Title: *Generators and integer points on the elliptic curve $y^2 = x^3 - nx$*

Abstract: Let E be an elliptic curve over the rationals $\mathbb{Q}$ given by $y^2 = x^3 - nx$ with a positive integer n. We are interested in integer points on E and generators for the Moedell-Weil group $E(\mathbb{Q})$.

Consider first the case where n is a perfect square. Assume that $n = N^2$ for a square-free integer N. Then, we show that if $E(\mathbb{Q})$ has rank one, there exist at most 17 integer points on E. Moreover, we show that for some parameterized N a point P can be in a system of generators for $E(\mathbb{Q})$ and completely determine the integer points in the group generated by the torsion points and the point P.

Secondly, consider the case where n is non-square, more precisely, where $n = s^4 + t^4$ for coprime positive integers s and t. It is known that the rank of $E(\mathbb{Q})$ is greater than or equal to two. We here show that if n is fourth-power-free, then the points $P_1 = (-t^2, s^2t)$ and $P_2 = (-s^2, st^2)$ can be in a system of generators for $E(\mathbb{Q})$. Furthermore, we prove that if n is square-free, then there exist at most nine integer points in the group Γ generated by the points P_1, P_2 and $(0,0)$. In particular, in case $n = s^4 + 1$ the integer points in Γ are completely determined.

Taka-aki Tanaka (Keio Univ.)

Title: *Algebraic independence of the values of Mahler functions with 'negative' transformations*

Abstract: Mahler's method gives algebraic independence results for the values of functions of several variables satisfying certain functional equations, called Mahler type functional equations, under the transformations of the variables represented as the multiplicative action of matrices with integer entries. In the Mahler's method, the matrices representing the transformations of the variables are restricted to nonnegative matrices; however, in a special case, one can admit having a negative entry. In this talk I will show the algebraic independence of the values of certain functions satisfying Mahler type functional equations under the transformation represented by a matrix including a negative entry by expressing those values as linear combinations of the values of ordinary Mahler functions.