PROGRAM FOR ICCGNFRT–2019

The four day conference will begin with a keynote talk on 16-th October, 2019 and end with a valedictory function on 19-th October, 2019. There will be 15 sessions consisting of one keynote, 7 plenary, 13 invited and 4 young scholar talks.

DAY-01 (October 16, 2019, WEDNESDAY)

TIME	SCHEDULE
8:50–9:50	REGISTRATION
9:50–10:00	INAUGURATION
	MORNING SESSION CHAIR PERSON: Prof. Tarlok Nath Shorey
10:00–11:00	KEYNOTE TALK: On the representation of integers by cyclotomic binary forms of large degree SPEAKER: Prof. Michel Waldschmidt, Institut de Mathématiques de Jussieu, France ABSTRACT: For each integer $d \geq 4$, we study the sequence of positive integers which are represented by one at least of the cyclotomic binary forms $\Phi_n(X, Y)$, with n a positive integer satisfying $\varphi(n) \geq d$. This is a joint work with Etienne Fouvry (to appear in Bulletin de la Société Mathématique de France, text in French), a continuation of a previous work with Claude Levesque and Etienne Fouvry (Representation of integers by cyclotomic binary forms, Acta Arithmetica, 2018, in English).
11:00–11:20	High Tea
	PRE-LUNCH SESSION CHAIR PERSON: Prof. Renate Scheidler
11:20–12:00	INVITED TALK: On the abelian group problem SPEAKER: Prof. Ayyadurai Sankaranarayanan, TIFR Mumbai, India ABSTRACT: We discuss Upper bound for the mean square of the error term related to the summatory function of the number of isomorphic abelian groups of order n up to x.
12:00–12:10	Discussion
12:10–12:50	INVITED TALK: The size function for imaginary cyclic sextic fields SPEAKER: Prof. Ha Thanh Nguyen Tran, Concordia University of Edmonton, Canada

TIME	SCHEDULE
	ABSTRACT: Arithmetic dynamics is a combination of dynamical systems and number theory. In this talk, we discuss the rational periodic points of polynomials with rational coefficients. We also discuss Morton and Silvermans uniform boundedness conjecture. It states that the number of periodic points of any rational function with rational coefficients is bounded by a constant depending only on the degree of the function. The conjecture is still unsolved even for quadratic polynomials.
13:00–14:30	LUNCH at guest house
	POST-LUNCH SESSION CHAIR PERSON: Prof. Ayyadurai Sankaranarayanan
14:30–15:30	PLENARY TALK: Constructing class groups of imaginary quadratic fields with large n-rank SPEAKER: Prof. Michael J. Jacobson, University of Calgary, Canada ABSTRACT: Constructing imaginary quadratic fields whose ideal class groups have large n-rank has proved to be a challenging practical problem, due in part to fact that we believe such examples to be very rare. One of the most successful methods for producing many fields of relatively small discriminant with large 3-rank is due to Diaz y Diaz; this was part of the method used by Quer to find 3 fields with 3-rank equal to 6 in 1987, which still stands as the current record. We describe generalizations to this method for constructing fields with large n-rank for an arbitrary integer $n \geq 3$, and practical enhancements to improve the efficiency of the search procedure. We present some preliminary numerical results, including the first known example of an imaginary quadratic field whose class group has 7-rank equal to 4.
15:30–15:50	Tea & Discussion
	EVENING SESSION CHAIR PERSON: Prof. Yasuhiro Kishi
15:50–16:30	INVITED TALK: p^r-Selmer companion modular forms SPEAKER: Prof. Somnath Jha, IIT Kanpur, India ABSTRACT: Given two elliptic curves E_1 and E_2 over a number field K, Mazur and Rubin have defined them to be n-Selmer companion if for every quadratic twist χ of K, the n-Selmer group of E_1^χ and E_2^χ over K are isomorphic. We will discuss an analogue of this for modular forms. This talk is based on a joint work with Sudhanshu Shekhar and Dipramit Majumdar
16:30–16:40	Discussion

TIME	SCHEDULE
16:40–17:10	YOUNG SCHOLAR TALK: Irreducibility of some polynomials SPEAKER: Dr. Anuj Jakhar ABSTRACT:
17:10–17:20	Tea at guest house
20:00–21:30	DINNER at guest house

DAY-02 (October 17, 2019, THURSDAY)

TIME	SCHEDULE
	MORNING SESSION CHAIR PERSON: Prof. Anupam Saikia
9:30–10:30	PLENARY TALK: A journey of cryptography in class groups of quadratic fields SPEAKER: Prof. Renate Scheidler, University of Calgary, Canada ABSTRACT: Cryptography in class groups of quadratic fields dates back to 1988, with the advent of the first Diffie-Hellman key style agreement protocol whose security resides in the intractability of extracting discrete logarithms in the class group of an imaginary quadratic field. Since then, the field has undergone a turbulent history. A host of other class group cryptosystems were put forward, founded on both the discrete log problem and the integer factorization problem. Following devastating breaks of the factoring-based schemes in 2009, the field made a come-back in 2015 with the advent of linearly homomorphic encryption in class groups of imaginary quadratic fields, which revived research in this area. Class groups also feature prominently in elliptic curve isogeny based cryptographic protocols. This talk tells the tumultuous story of class group based cryptography, from its beginnings some 30 years ago to ongoing research on quantum resistant schemes.
10:30–10:50	Tea & Discussion
	PRE-LUNCH SESSION CHAIR PERSON: Prof. Kotyada Srinivas
10:50–11:30	INVITED TALK: A note on the construction and enumeration of Euclidean self-dual skew-cyclic codes SPEAKER: Prof. Intan Muchtadi-Alamsyh ABSTRACT: Skew-cyclic codes or θ-cyclic codes over finite fields are generalization of cyclic codes over finite fields. Here, θ is an automorphism in the corresponding finite fields. In this talk, we will discuss the construction and enumeration of self-dual skew-cyclic or θ-cyclic codes when $(n, \lvert\theta\rvert) = 1$, where $\lvert\theta\rvert$ is the order of the automorphism θ.
11:30–11:40	Discussion
11:40–12:20	INVITED TALK: On some properties concerned with the continued fraction expansion of $\sqrt{d}$ with even period, II SPEAKER: Prof. Yasuhiro Kishi, Aichi University of Education, Japan

TIME	SCHEDULE
	ABSTRACT: For an even positive integer ℓ, let d_ℓ be the smallest integer d such that the minimal period of the simple continued fraction expansions of $\sqrt{d}$ is equal to ℓ, where d runs through non-square positive integers with $d \equiv 2, 3 \pmod 4$. In ICCGNFRT-2017, we discussed some properties of partial quotients of the continued fraction expansion of $\sqrt{d_\ell}$, including the class number of real quadratic field $\mathbb{Q}(\sqrt{d_\ell})$ is equal to 1 for each even positive integer ℓ with $2 \leq \ell \leq 73478$. In this talk, we give some relations between them.
12:20–12:30	Discussion
12:30–13:10	INVITED TALK: Root numbers and Iwasawa Invariants of elliptic curves SPEAKER: Prof. Sudhanshu Shekhar, IIT Kanpur, India ABSTRACT: Given two elliptic curves E_1 and E_2 defined over the field of rational numbers, with good reduction at an odd prime p and equivalent mod p Galois representations, we compare the parity of p-Selmer rank and root numbers of E_1 and E_2 over number fields.
13:10–14:30	LUNCH at guest house
	POST-LUNCH SESSION CHAIR PERSON: Prof. Michael J. Jacobson
14:30–15:30	PLENARY TALK: Non-Galois cubic number fields with exceptional units SPEAKER: Prof. Stéphane Louboutin, Aix-Marseille Université, France ABSTRACT: An algebraic unit ε is called a special unit if $\varepsilon - 1$ is also a unit. Assume moreover that $\mathbb{Q}(\varepsilon)$ is non-Galois totally real cubic number field. Then ε and $\varepsilon - 1$ are multiplicatively independent and it is known that $\{\varepsilon, \varepsilon - 1\}$ is a system of fundamental units of the cubic order $\mathbb{Z}[\varepsilon]$. Now, the unit index j_ε of the groups of units generated by -1, ε and $\varepsilon - 1$ in the group of units of the ring of algebraic integers of $\mathbb{Q}(\varepsilon)$ is finite. V. Ennola conjectured that j_ε is always equal to 1, i.e. that $\{\varepsilon, \varepsilon - 1\}$ is always a system of fundamental units of $\mathbb{Q}(\varepsilon)$. Fix an algebraic closure of $\mathbb{Q}$. Here we prove that for any prime p there are only finitely many cases for which p divides j_ε and explain how this result makes Ennola's conjecture very reasonable for its possible exceptions would be few and far between.
15:30–15:50	Tea & Discussion
	EVENING SESSION CHAIR PERSON: Prof. Benjamin Kane
15:50–16:30	INVITED TALK: Iwasawa invariants of p-adic measures

TIME	SCHEDULE
	SPEAKER: Prof. Rupam Barman, IIT Guwahati, India ABSTRACT: We introduce Iwasawa invariants of p-adic measures on $(\mathbb{Z}_p)^n$ and their Gamma transforms. We prove a relation between the Iwasawa lambda invariants of a p-adic measure and it's Gamma transform. We also determine p-adic properties of certain Mahler coefficients by exploiting some combinatorial identities. Finally, we give some applications of our main result.
16:30–16:40	Discussion
16:40–17:10	YOUNG SCHOLAR TALK: Lower bound for class number of certain real quadratic fields SPEAKER: Mr. Mohit Mishra, Harish-Chandra Research Institute, India ABSTRACT: Let d be a square-free positive integer and $h(d)$ the class number of the real quadratic field $\mathbb{Q}(\sqrt{d})$. In this paper we give an explicit lower bound for $h(n^2+r)$, where $r = 1, 4$, and also establish an equivalent criteria to attain this lower bound in terms of special value of Dedekind zeta function. Applying our results, we obtain some criteria for class group of prime power order to be cyclic. Our bounds enable us to reduce the real quadratic families considered in Chowla and Yokoi's conjecture to comparatively smaller subfamily. We also give an equivalent criteria for having an alternate proof of both the conjectures.
17:10–17:20	Tea at guest house
20:00–21:30	DINNER at guest house

DAY-03 (Otober 18, 2019, FRIDAY)

TIME	SCHEDULE
	MORNING SESSION CHAIR PERSION: Prof. Michel Waldschmidt
9:30–10:30	PLENARY TALK: Attempting a non-abelian generalization of Herbrand-Ribet theorem SPEAKER: Prof. Dipendra Prasad, IIT Bomaby, India ABSTRACT: Herbrand-Ribet theorem in the title refers to p-class groups of cyclotomic number fields in terms of p-divisibility of certain L-values. We discuss one generalisation of this theorem involving class group of field generated by p-torsion points of an elliptic curve over $\mathbb{Q}$, with some concrete questions.
10:30–10:50	Photo Session, Tea & Discussion
	PRE-LUNCH SESSION CHAIR PERSON: Prof. Valerio Talamanca
10:50–11:30	INVITED TALK: Dynamical systems over finite fields SPEAKER: Prof. Chatchawan Panraksa, Mahidol University, Thailand ABSTRACT: The iteration of rational functions over number fields has gained steady interest in the past three decades. Recently, the dynamical systems over finite fields (DFF) have recently attracted researchers from dynamical systems and number theory. This is due to intrinsic interests and applications in related fields. This talk will discuss the dynamical systems of quadratic polynomials over finite fields. It is related to joint work with Atsanon Wadsanthat.
11:30–11:40	Discussion
11:40–12:20	INVITED TALK: Euclidean multi-quadratic fields SPEAKER: Prof. Kotyada Srinivas ABSTRACT: In this talk we shall discuss the Euclidean nature of number fields of the form $\mathbb{Q}(\sqrt{m_1}, \sqrt{m_2}, \cdots, \sqrt{m_l}), l \geq 2$.
12:20–12:30	Discussion
12:30–13:10	INVITED TALK: Selmer group associated to Chow group of an abelian variety and weak Mordell-Weil theorem SPEAKER: Dr. Kalyan Banerjee, Harish-Chandra Research Institute

TIME	SCHEDULE
	ABSTRACT: The Selmer group and the Tate-Shafarevich group of an elliptic curve or more generally of an abelian variety defined over a number field are very interesting and important in the study of arithmetic of abelian varieties. Long standing conjecture says that the Tate-Shafarevich group is finite for any abelian variety defined over a number field. The finiteness of the Selmer group is known and from this the weak Mordell-Weil theorem for an abelian variety can be deduced. In this talk we are going construct the Selmer group and the Tate-Shafarevich group for the Chow group of an abelian variety. We will show that the Selmer group of the Chow group is finite and we prove an analog of weak Mordell-Weil theorem for Chow groups. Time permitting I will also relate this result to the n-divisibility questions of the class group of number fields.
13:10–14:30	LUNCH at guest house
	POST-LUNCH SESSION CHAIR PERSON: Prof. Dipendra Prasad
14:30–15:30	PLENARY TALK: On the Iwasawa μ-invariants of supersingular elliptic curves SPEAKER: Prof. Anupam Saikia, IIT Guwahati, India ABSTRACT: We explore the relation between the Iwasawa invariants μ^+ and μ^- associated respectively with the plus and the minus Selmer groups of two elliptic curves E_1 and E_2 over $\mathbb{Q}$ having isomorphic Galois representations $E_1[p^r] \cong E_2[p^r]$ at a prime p of supersingular reduction. We prove that $\mu^{\pm}(E_1) = \mu^{\pm}(E_2)$ if either is less than r and $\mu^{\pm}(E_1), ^{\pm}(E_2) \geq r$, if either is greater than or equal to r.
15:30–15:50	Tea & Discussion
	EVENING SESSION CHAIR PERSON: Prof. Rupam Barman
15:50–16:30	INVITED TALK: On sequences of integers of quadratic fields and relations with Artin's primitive root conjecture SPEAKER: Prof. Nihal Bircan Kaya, Cankiri Karatekin University, Turkey

TIME	SCHEDULE
	ABSTRACT: I will consider the integers α of the quadratic field $\mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z}$ is square-free integer. Using the embedding into $\mathrm{GL}(2,\mathbb{R})$ we obtain bounds for the first $\nu \in \mathbb{N}$ such that $\alpha^\nu \equiv 1 \bmod p$. More generally, if $\mathcal{O}_f$ is a number ring of conductor f, we study the first integer $n = n(f)$ such that $\alpha^n \in \mathcal{O}_f$. We obtain bounds for $n(f)$ and for $n(fp^k)$. We allow any norm $N(\alpha) \neq 0$. The case where α is the fundamental unit in a real quadratic number field is of special interest. We also study a certain probability distribution suggested by the numerical results. In the second part of my talk I will indicate in details how my results relate to Artin primitive root type problems over quadratic fields.
16:30–16:40	Discussion
16:40–17:10	INVITED TALK: On the class number of some real quadratic number fields SPEAKER: Prof. Claude Levesque, University of Laval, Canada ABSTRACT: I plan to speak on some results related to the class number of certain families of real quadratic fields.
18:30-20:00	CULTURAL EVENT at auditorium
20:00-21:30	CONFERENCE BANQUET DINNER at guest house

DAY-04 (OCTOBER 19, 2019, SATURDAY)

TIME	SCHEDULE
06:30–09:00	Boat trip towards SANGAM - the confluence of three holy rivers the Ganga, Yamuna and Saraswati
	MORNING SESSION CHAIR PERSION: Prof. Michel Waldschmidt
10:30–11:30	PLENARY TALK: Irreducibility of Laguerre polinomials SPEAKER: Prof. Tarlok Nath Shorey ABSTRACT:
11:30–11:50	Tea & Discussion
	PRE-LUNCH SESSION CHAIR PERSON: Prof. Chatchawan Panraksa
11:50–12:30	INVITED TALK: Symmetries for heights on split tori SPEAKER: Prof. Valerio Talamanca, Roma Tre University, Italy ABSTRACT: We will discuss, in a few examples, the group of symmetries for heights associated to representations on a split tori. We will also discuss the validity of the Northocott's theorem for these heights.
12:30–12:40	Discussion
12:40–13:10	YOUNG SCHOLAR TALK: Arithmetic properties of the integer partitions with even parts below odd parts and modular forms SPEAKER: Dr. Chiranjit Ray ABSTRACT: In this talk, we will discuss some arithmetic properties and distribution of Andrews' integer partitions with even parts below odd parts. We also discuss the parity of this partition function in any arithmetic progression. We use the arithmetic properties of modular forms and Hecke eigenforms to get these results. This is a joint work with Dr. Rupam Barman.
13:00–14:30	LUNCH
	POST-LUNCH SESSION CHAIR PERSON: Prof. Stéphane Louboutin
14:30–15:00	YOUNG SCHOLAR TALK: Class groups in Kummer towers SPEAKER: Dr. Jianing Li, University of Science and Technology, China

TIME	SCHEDULE
	ABSTRACT: I will talk about some explicit results on the ℓ-class group of $K_{n,m} = \mathbb{Q}(\sqrt[\ell^n]{p}, \mu_{\ell^m})$ where ℓ and p are two primes. More precisely, I will state a general result on odd regular ℓ. In the case $\ell = 2$, we determine 2-class group of $K_{n,m}$ for all n, m when p is congruent to 3,5 modulo 8, generalizing the results of Parry about the 2-divisibility of the class number of $K_{2,0}$. I will try to explain the concept of norm-compatible tower which is important to the proof. If time permits, I will go through another proof which is by some stable results of class groups in cyclic extensions. This is a joint work with Y. Ouyang, Y. Xu and S. Zhang.
15:00–16:00	PLENARY TALK: Ternary quadratic forms with congruence conditions and Hurwitz class numbers for imaginary quadratic orders SPEAKER: Prof. Benjamin Kane, Hong Kong University, Hong Kong ABSTRACT: In this talk, we will discuss a question posed by Petersson about coefficients of certain theta functions for quadratic forms with congruence conditions. Namely, he claimed that the coefficients of certain such theta functions had formulas as some sort of Hurwitz class numbers. We revisit his claim with a modern perspective and explain the source of these theta functions. Using that perspective, we find a large number of other forms satisfying such formulas. This is based on joint work with Kathrin Bringmann.
16:05–16:20	VALIDICTORY FUNCTION at auditorium
16:20-17:40	HIGH TEA at guest house
20:00–21:30	DINNER at guest house