INFOMAT

August 2014

SE CHRISTIAN SKAU OG MARTIN RAUSSEN I SAMTALE MED YAKOV SINAI PÅ KUNNSKAPSKANALEN, NRK2, LØRDAG 23. AUGUST KL. 1710-1815

Abelprisen deles ut hvert år av Det Norske Videnskaps-Akademi for fremragende vitenskapelig arbeid i matematikk, og den er på 6 mill.kroner. I år var det den russiske matematikeren Yakov G. Sinai som fikk prisen for sitt vesentlige bidrag til dynamiske systemer, ergodeteori og matematisk fysikk. H.K.H. Kronprinsen overrakte prisen til Yakov Sinai under en høytidlig seremoni i Universitetets aula. Professorene Christian Skau og Martin Raussen møtte prisvinneren til en samtale om hans matematiske forskning. Produsert av UniMedia, Universitetet i Oslo.

INFOMAT kommer ut med 11 nummer i året og gis ut av Norsk Matematisk Forening. Deadline for neste utgave er alltid den 15. i neste måned. Stoff til INFOMAT sendes til

infomat at math.ntnu.no

Foreningen har hjemmeside http://www.matematikkforeningen.no/INFOMAT
Ansvarlig redaktør er Arne B. Sletsjøe, Universitetet i Oslo.

NYHETER

Matematisk kalender

2014:
September:
15.-19. *Stochastics of Environmental and Financial Economics*, DNVA, Oslo
Oktober:
23.-24. *Mathematics video-tutorial production* (MathRIC), Bergen
November:
6.-7. *Nasjonalt algebramøte*, Oslo
23.-24. *MathRICs årskonferanse*, Trondheim

MATRIC – CENTRE FOR RESEARCH, INNOVATION AND COORDINATION OF MATHEMATICS TEACHING

Kommende arrangementer:
23.-24. oktober: Høgskolen i Bergen, Workshop: «Mathematics video-tutorial production». Dette er et arrangement Høgskolen i Bergen ogMatRIC samarbeider om.
27.-28. november: MathRICs første årskonferanse, Trondheim, Temaet for konferansen er matematikkundervisning på universitets- og høyskolenivå. Professor Tom Lindstrøm vil holde hovedforedraget med tittel: What does it mean to understand mathematics? A few questions and no answers. MatRICs konferanse vil til dels overlappe med Matematikksenterets novemberkonferanse og det vil være to felles foredrag med henholdsvis Tim Rowland og Jo Røislien. Konferansen vil i tillegg bestå av workshops basert på de tre arbeidsgruppene i MatRIC: Simulation Working Group, Digital Assessment and Video-teaching Working Group and Mathematical Modeling Working Group.
Konferansen er gratis og MatRIC dekker en overnatting. Vennligst se program og lenke til påmelding på uia.no/MatRIC.
For mer informasjon om noen av de ovennevnte arrangementene kontakt line.e.malde@uia.no
For mer informasjon om senteret se: matric.no

Utlysninger

2-ÅRIG POSTDOC I ANVENDT MATEMATIKK VED NMBU PÅ ÅS.

Det er ledig en 2 - årig postdoc stilling i anvendt matematikk ved Norges miljø- og biovitenskapelige universitet (NMBU):
To qualify for the position, you must at least have a PhD degree in applied mathematics or mathematics. First of all, applicants with documented research in dynamical systems theory, functional analysis and computational mathematics will be given preference. Secondly, emphasis will be put on documented research in mathematical neuroscience and/or gene regulatory networks. Thirdly, documented research collaboration with scientists in systems-biology, computer science, physics and engineering sciences will also be taken into account in the assessment.
Søknadsfrist: **1 september 2014**
http://www.jobbnorge.no/ledige-stillinger/stilling/102574/postdoctoral-fellow-in-applied-mathematics-refno-14-02640

Nyheter

UIOs FORSKNINGSPRIS TIL BERNT ØKSENDAL

Bernt Øksendal ved Matematisk institutt, UiO får UiOs forskningspris for 2014. Prisen deles ut i forbindelse med universitetets årsfest 2. september.

NYHETER

LOREN DAVID OLSON (1942-2014)

Loren D. Olson døde uventet 22. juni i Tromsø. En pionér i matematikk- og realfagsmiljøet ved Universitetet i Tromsø, og en god venn, og avholdt kollega, er gått bort.

Olson ble født i Grand Forks, North Dakota i 1942 og vokste opp i et miljø i Midt-Vesten med solide norske røtter. Han studerte ved Harvard University utenfor Boston, og fullførte sin bachelorgrad i 1964. Så seint som i juni 2014 deltok han i en jubileumstilstelning for kullet sitt der, noe han satte stor pris på. Doktorgradsstudiene gjennomførte han i New York, der han mottok sin Ph.D.-eksamen ved Columbia-universitetet i 1968. Fra 1968 var Olson Instructor ved University of California, Berkeley, inntil han i 1970 fant vegen til Norge, der han bodde og arbeidet resten av sitt liv.

Fra barndommen hadde Loren lært et norsk basert på dialektene i Hallingdal og Valdres på 1800-tallet. Da han kom til Norge, lærte han seg også raskt «bokmålsnorsk», som han snart behersket til nær fullkommenhet.

I perioden 1970-75 var Olson ansatt som matematiker ved Universitetet i Oslo og Universitetet i Bergen, og fra 1975 var han professor i rein matematikk ved Universitetet i Tromsø. Her ble han fram til 2013 da han gikk av med pensjon og siden var professor emeritus samme sted.

Gjennom sine arbeider seint på 60-tallet og på 70-tallet etablerte Olson seg som en kapasitet innen tallteori og teori for elliptiske kurver, disipliner som i utgangspunktet er svært abstrakte og teoretiske, men som i de siste tiåra har fått stor betydning for kryptografi og datasikkerhet. Dette var fagfelt som Olson siden interesserte seg sterkt for, og gjennom sitt store internasjonale kontaktnett skaffet han matematikkmiljøet i Tromsø betydelige impulser. Her veiledet han, særlig på 80- og 90-tallet, flere doktorgradsstudenter, og en rekke hovedfagsstudenter. Loren Olson var en høyt verdsatt medarbeider og kollega. Han viet hoveddelen av sitt yrkesaktive liv til å bygge opp og drive fagmiljøet i matematikk ved Universitetet i Tromsø.

Ragnar Soleng og Trygve Johnsen,
Institutt for matematikk og statistikk,
Universitetet i Tromsø – Norges arktiske universitet.

ELLIPTISK KURVE-KRYPTOGRAFI

(Kilde: Wikipedia)

The use of elliptic curves in cryptography was suggested independently by Neal Koblitz and Victor S. Miller in 1985. Elliptic curve cryptography algorithms entered wide use in 2004 to 2005.

Public-key cryptography is based on the intractability of certain mathematical problems. Early public-key systems are secure assuming that it is difficult to factor a large integer composed of two or more large prime factors. For elliptic-curve-based protocols, it is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is infeasible — this is the "elliptic curve discrete logarithm problem" or ECDLP. The entire security of ECC depends on the ability to compute a point multiplication and the inability to compute the multiplicand given the original and product points. The size of the elliptic curve determines the difficulty of the problem.

The primary benefit promised by ECC is a smaller key size, reducing storage and transmission requirements, i.e. that an elliptic curve group could provide the same level of security afforded by an RSA-based system with a large modulus and correspondingly larger key – e.g., a 256-bit ECC public key should provide comparable security to a 3072-bit RSA public key (see key sizes below).

NYHETER

ÅRETS FIELDS-MEDALJISTER

FIELDS MEDAL (recognizing outstanding mathematical achievement), recipients are listed in alphabetical order of last names:
- ***Artur Avila*** of CNRS Paris (France) and IMPA (Brasil) *for his profound contributions to dynamical systems theory, which have changed the face of the field, using the powerful idea of renormalization as a unifying principle.*
- ***Manjul Bhargava*** of Princeton University (USA) *for developing powerful new methods in the geometry of numbers, which he applied to count rings of small rank and to bound the average rank of elliptic curves.*
- ***Martin Hairer*** of Warwick University (UK) f*or his outstanding contributions to the theory of stochastic partial differential equations, and in particular for the creation of a theory of regularity structures for such equations.*
- ***Maryam Mirzakhani*** of Stanford University (USA) *for her outstanding contributions to the dynamics and geometry of Riemann surfaces and their moduli spaces.*

ROLF NEVANLINNA PRIZE (honoring distinguished achievements in mathematical aspects of information science):
- ***Subhash Khot*** of New York University (USA) *for his prescient definition of the "Unique Games" problem,and leading the effort to understand its complexity and its pivotal role in the study of efficient approximation of optimization problems; his work has led to breakthroughs in algorithmic design and approximation hardness, and to new exciting interactions between computational complexity, analysis and geometry.*

CARL FRIEDRICH GAUSS PRIZE (for outstanding mathematical contributions with significant impact outside of mathematics):
- ***Stanley Osher*** of University of California (USA) *for his influential contributions to several fields in applied mathematics, and for his far-ranging inventions that have changed our conception of physical, perceptual, and mathematical concepts, giving us new tools to apprehend the world.*

CHERN MEDAL (awarded to an individual whose accomplishments warrant the highest level of recognition for outstanding achievements in the field of mathematics):
- ***Phillip Griffiths*** of Institute of Advanced Studies (USA) *for his groundbreaking and transformative development of transcendental methods in complex geometry, particularly his seminal work in Hodge theory and periods of algebraic varieties.*

LEELAVATI PRIZE, sponsored by Infosys (for outstanding contributions to public outreach in mathematics by an individual):
- ***Adrian Paenza*** of Buenos Aires University (Argentina) *for his decisive contributions to changing the mind of a whole country about the way it perceives mathematics in daily life, and in particular for his books, his TV programs, and his unique gift of enthusiasm and passion in communicating the beauty and joy of mathematics.*

BREAKTHROUGH PRIZE IN MATHEMATICS

Five Winners Receive Inaugural Breakthrough Prize In Mathematics:

Simon Donaldson (Stony Brook University and Imperial College London),
for the new revolutionary invariants of 4-dime nsional manifolds and for the study of the relation between stability in algebraic geometry and in global differential geometry, both for bundles and for Fano varieties.

Maxim Kontsevich, (Institut des Hautes Études Scientifiques, France),
f*or work making a deep impact in a vast variety of mathematical disciplines, including algebraic geometry, deformation theory, symplectic topology, homological algebra and dynamical systems.*

Jacob Lurie (Harvard University), *for his work on the foundations of higher category theory and derived algebraic geometry; for the classification of fully extended topological quantum field theories; and for providing a moduli-theoretic interpretation of elliptic cohomology.*

Terence Tao (University of California, Los Angeles), *for numerous breakthrough contributions to harmonic analysis, combinatorics, partial differential equations and analytic number theory.*

Richard Taylor, (Institute for Advanced Study), *for numerous breakthrough results in the theory of automorphic forms, including the Taniyama-Weil conjecture, the local Langlands conjecture for general linear groups, and the Sato-Tate conjecture.*

The Breakthrough Prizes in Mathematics complement the Breakthrough Prizes in Fundamental Physics, which were inaugurated in 2012, and the Breakthrough Prizes in Life Sciences, which were inaugurated in 2013.
In future years, there will be one award in mathematics, one award in physics, and six in life sciences. Each of the eight annual awardees will receive USD$3,000,000, as in the inaugural prizes. Funding for the Breakthrough Prizes is provided jointly by Russian Internet billionaire Yuri Milner, who founded the prizes, and Facebook founder Mark Zuckerberg. The intent is to establish awards of stature comparable to or exceeding that of the Nobel prizes.