ICMAT
INSTITUTO DE CIENCIAS MATEMÁTICAS

Quarterly newsletter
First quarter 2016
CSIC - UAM - UC3M - UCM

EDITORIAL

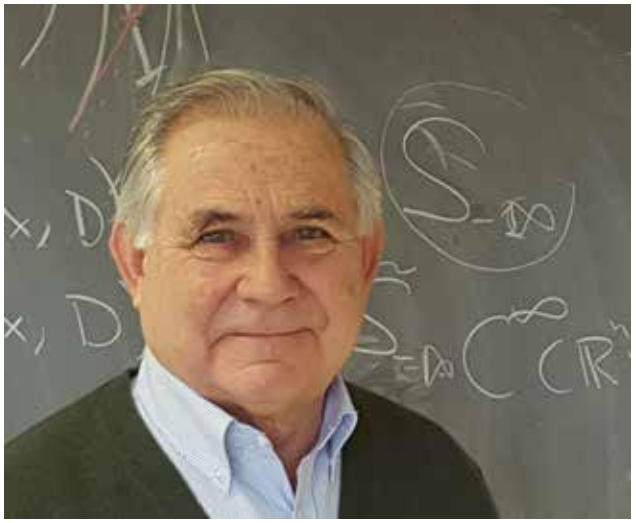
Vita académica, vita beata

According to a well-known saying attributed to Confucius, it is not appropriate to speak well or badly about oneself, because if you did it, nobody would believe you in the first case, while in the second case they would agree with you completely. However, in what follows I am going to ignore this advice, while at the same time attempting to avoid adjectives, either flattering or derogatory, regarding events that have marked my university career and which I believe may have a some interest above and beyond a mere personal anecdote. I also believe they may be appropriate at a time when I have just taken up my position as director of the ICMAT.

Although I took part in the meetings just prior to the creation of the Institute, around 2003-2004, I have belonged to the faculty since just before we moved into this magnificant building that we now occupy in usufruct. Those who come here often will have noticed that I am usually here in the mornings and give my classes in the Autonomous University of Madrid (UAM) Department of Mathematics. However, I spend the afternoons at the ICMAT, where I have enjoyed many interesting seminars, have imparted courses on analysis and fluid mechanics, have conducted research and collaborated on various articles. And sometimes I even have suprised myself by telling anecdotes in the cafeteria to the younger students about people in our profession who I have known throughout my career.

In private, and in public, as those who have read my articles in the press will know, I have made it clear that the work carried out at the Institute during its short history has been magnificent, almost miraculous. It is enough to mention the number of ERC projects awarded, the obtention and renewal of Severo Ochoa award, and the not inconsiderable number of quality theorems developed and subsequently published in leading scentific journals. I believe it is opportune to draw attention to this again, while at the same time to thank former directors of the ICMAT, Manuel de León and Rafael Orive, for their tireless and fruitful efforts, without which these splendid facilities we now enjoy would never have existed.

The research institutes have been an important and sometimes decisive factor in the development of mathematics, and have become a cohesive and driving force in the research work conducted in the university departments in their respective geographial areas. The ICMAT is a joint endeavour with the *Consejo Superior de Investigaciones Científicas* (CSIC) and the Autonomous, Complutense and Carlos III Universities in Madrid. One of our most important challenges is to facilitate and perfect interaction between all the components in the running of the Institute.


ICMAT

Antonio Córdoba

CONTENTS

With the Carlos III University, which is the youngest of the four institutions, I have had only intermittent contact, such as giving talks or forming part of the examination board. As regards the other three, they have played a significant role in my academic career. I studied for my degree at the Complutense University of Madrid (UCM) during the fascinating and eventful period around 1968. I was a researcher at the CSIC for three years (1976-78), a post I combined with that of professor at Princeton University. I was then for a short period professor at the UCM, where among other tasks I supervised the thesis of my first PhD student. Finally, in late 1979, I took up the position of Chair at the Autonomous University of Madrid (UAM).

Throughout my career at different academic institutions, I have had the occasion to observe two vices that poison university life in Spain. For reasons of simplification, I will call these vices "envy" and "quid pro quo", which I believe it is necessary at all costs to avoid in our Institute. It is a cliché to say that envy is the Spanish vice par excellence. It was José Luis Borges who remarked that the Spanish, when describing something that is very good, often say that it is enviable. Personally, I do not believe in such stereotypes, but I do believe in the current university version consisting in not appointing anyone who might leave you in the shade. From my experience in the USA, I learnt that such a vice is penalized there; that appointing anyone not best suited to the post undermines overall expectations, while on the other hand surrounding oneself with the best makes us all better – in status, in curriculum and in salary. This is a policy that the ICMAT has always tried to pursue, by attracting the best talent no matter where it comes from, and this is what I fully intend to continue.

To a certain extent, "quid pro quo" can be beneficial; it stimulates cooperation and a certain social cohesion, but in the university sphere, when it is carried too far, it leads to cliques and coteries, *hortus conclusus*; bosses who you have to applaud or face the consequences, who at the same time offer protection and support in exchange for promotion to membership of the clan.

In general, mathematical research is also a social activity insofar as the decision to explore a particular subject or follow a particular approach is often the result of the interest and stimulus provided by others. Communication is the laboratory of mathematicians, whose research work normally involves the assistance and constructive criticism from different colleagues. For all these reasons, ongoing activity often requires funding for trips and stays at centers of excellence where scientific contacts are made and cemented.

Generally speaking, the needs of mathematicians are affordable and attainable; time for research work, and three types of infrastructure: libraries, means of computation, and technical and administrative resources. Unfortunately, such straightforward requirements are sometimes lacking in day-to-day practice. We need the adequate administrative staff to help us in the many routine and bureaucratic tasks we are required to perform, in the application for projects, for example, as well as in their justification and management. The ICMAT seeks to create the ideal environment for such a venture, an intellectual community of thinkers in which management is conducted in such a way that it does not stand in the way of progress. Nevertheless, to paraphrase Borges, and let no one take this as a reproach or a shedding of tears, but rather as a simple statement of reality, that since taking up my position as director I have had very little time for my own research work, because I have been too busy making sure that others might enjoy the basic conditions for pursuing their own. Whatever the case, providing it ensures that our Institute is able to maintain the excellent results it has so far achieved in its short history, I consider it time well spent.

May truth and beauty accompany you always.

Antonio Córdoba

Director

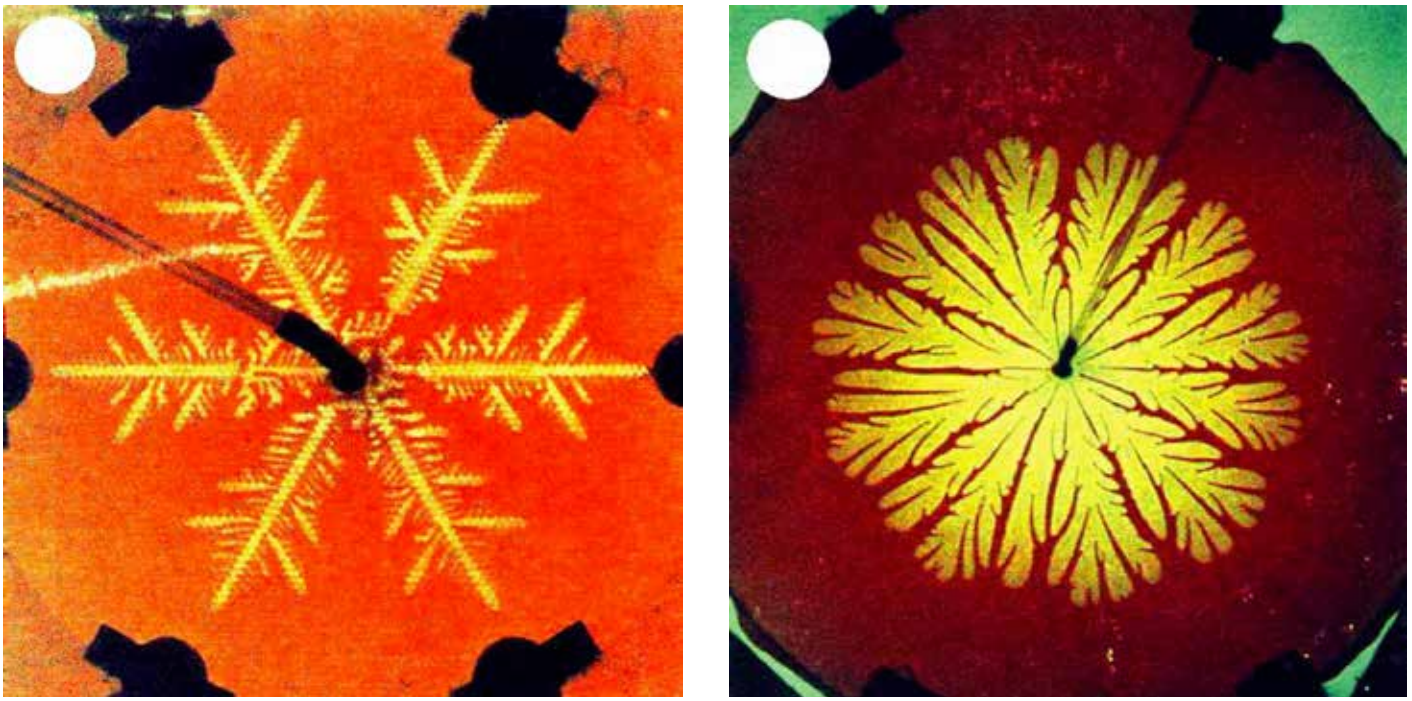
Antonio Córdoba is a Professor of Mathematical Analysis at the Autonomous University of Madrid and has been a member of the ICMAT (Instituto de Ciencias Matemáticas) since it first began. In 2011 he was awarded the Julio Rey Pastor National Prize for Mathematics and Communication Sciences. He gained his degree from the Complutense University of Madrid and completed his doctorate at the University of Chicago. He has been a professor at the Universities of Princeton, Chicago and Minnesota and a member of the Princeton Institute for Advanced Study. He is the author of more than 100 research papers as well as various books, essays and outreach articles.

ICMAT

REPORTAGE: International workshop in mathematical biology at the ICMAT

THE MICROSCOPE IS MATHEMATICS

A profound knowledge of biological mechanisms enables future irreparable threats to be anticipated and avoided, such as the consequences of climate change and the disappearance of species; it provides a faster alternative for the development of pharmaceutical drugs; it personalizes the fight against cancer, and helps in the effective management of fishing resources. To that end, mathematical biology provides a tool capable of modelling living systems and thereby to understand the processes sampled as well as testing hypotheses with simulations. It is also able to go further in the observation of reality when the information in a given sample is too little or too great. This symbiosis between the two sciences is in the ascent and promises to furnish excellent results.



Ben-Jacob & Garik 1990

Basic symmetric patterns observed in the nature

Elvira del Pozo Campos. In a recent interview, the director of the prestigious Weizmann Institute of Science (Israel), Daniel Zajfmann, states that: "The next scientific revolution will come from a multidisciplinary group of scientists". He is referring to the collaboration between computation, mathematics, physics and biomedicine as one of the most promising fields in the fight against cancer. This is one of the research lines in mathematical biology, a discipline that is on the rise and to which the workshop Mathematical Perspectives in Biology, held in February of this year at the *Instituto de Ciencias Matemáticas* (ICMAT), was dedicated.

At this meeting, models were presented on which national and international research teams are working in fields such as the development of new drugs, the spread of epidemics, the effects of climate change and over-fishing in biodiversity. As one of the organizers of the conference and ICMAT researcher, Kurusch Ebrahimi-Fard, explains: "The aim was to determine the mathematical research lines related with biology and to promote dialogue between the different centers".

This scientific area, in which natural processes are studied by using mathematics as a tool, is currently enjoying a rapid expansion. As Ebrahimi-Fard says, "Biology can stimulate the development of new mathematics, just as physics did in the last century. Mathematics is the new microscope in biology". Last year he was also in charge of a BBVA Foundation project on mathematical methods for ecology and industrial management.

Kurusch Ebrahimi-Fard

Instead of magnifying all the details, a microscope reveals the most important information. Tomás Alarcón, an expert in the modelling of tumors at the *Centre de Recerca Matemàtica* Computational and Mathematical Biology Unit (CRM), says that the work of a mathematician in this field is "to sift through every detail of all the literature published in Biology and boil it down to the basics and the similarities". The result is that this process "generates equations that capture the essential features of reality and leaves aside what is superfluous", adds Antonio Gómez Corral, ICMAT member and a professor at the Complutense University of Madrid (UCM). Biology has currently moved from describing nature to attempting to understand how it functions. A model provides indicators, a framework of comparison and an overall vision.

"Mathematical biology generates equations that capture the essential features of reality and leaves aside what is superfluous"

However, there was not always such harmony between the two sciences: since their first collaboration in the late 18th century, biologists have criticized mathematical results as being unreliable, says Gómez Corral, because they regarded the models as a clumsy copy of complex living systems. Another organizer of the workshop and also a UCM researcher, Francisco Cao, says that it was only a few decades ago when more robust mathematical tools – mainly stochastic ones – began to be used in fields such as ecology and population analysis. He also states that "their use at a celular and molecular level is rather more recent".

Technological advances enable measurements to be made that were not possible before, which constitutes a data source that allows a greater acquisition of knowledge. As Cao explains: "This has acted as a spur for mathematics to create new tools to help in the understanding of the enormous amount of data being measured". In his opinion, "since in the natural sciences every problem is singular, the mathematics employed is extremely varied".

Mathematics can also resolve the inverse problem: when there is not sufficient information. It is impossible to sample everything in the necessary detail and in all parts of the world, but mathematics completes the image. Bernt-Erik Sæther, biologist at the Norwegian University of Science and Technology (NTNU), points out that: "The algorithms extrapolate and generate values where there is no real measurement".

Asocial fish

96% of Mediterranean fish stocks (individual fish whose size and species allow them to be fished) managed by the European Union are overfished, and seven out of ten of those in the Atlantic region fail to comply with the sustainability recommendations, according to the New Economics Foundation (NEF) and Oceana. Given this situation, the EU has set the target of meeting the quotas in all the fishing grounds by 2002, while Oceana is demanding "immediate emergency closures". What is the reason for such urgency? As mathematician at the NTNU, Steinar Engen, explains: "It's not easy to recover fish populations simply by stopping fishing".

In an article he published jointly with Sæther, Engen found that "intensive fishing affects the genetics of fish populations and leads to permanent consequences in these populations". Certain individuals respond better to conditions of stress and these are the ones that survive. When pressure on the fishing ground is lifted "the consequences are not immediately evident", because the organisms that remain may not be the best adapted to the density of large populations.

"The algorithms extrapolate and generate values where there is no real measurement"

The permanent loss of species, like the impact on their genetics as well as the changes and interactions between them, "may take a long time to become manifest, and by then the effects may well be irreversible", says Sæther. It is here where mathematical models can make a contribution to this matter, since they enable us to foresee the evolution of a natural system, to detect problems before it's to late and thus design preventative measures", says another organizer of the event, Steven Gray, professor of computational engineering at the Old Dominion University (USA): "Everybody who eats is necessarily involved in these things".

Elephants, mice and phytoplankton

A further function of mathematical tools is that they "enable us to verify whether the perception of observers and the hypotheses they put forward are correct", states Emilio Marañón, a researcher with the Universidad of Vigo Department of Ecology and Animal Biology. His team has shown that, contrary to what was believed before, the so-called *mouse to elephant curve* is not universal. This law establishes an inverse relation between the size of an individual and the speed at which it grows. Marañón explains that, to date, it was regarded as valid for all animal species, but it is now known that it is not valid for phytoplankton.

"Small algae and large algae grow more or less a the same rate; it's the medium-sized algae that grow more quickly". This discovery may have remained as little more than a wildlife curiosity, were it not for the fact that these microscopic plants play an important role in the ecological balance of the Planet. They form the basis of the food chain in oceans, says Marañón, and produce half the oxigen released annually into the atmosphere. Knowledge of how they function can provide us with indicators for detecting changes in the environment, such as acidification of the seas, as well as helping us to design strategies for preserving biodiversity.

"It's not easy to recover fish populations simply by stopping fishing"

In this case, it was the observations that indicated that the model that was valid for "large animals" could not be extrapolated to these marine microorganisms. However, in Marañón's opinion, this is far from being a step backwards: "This deviation between the results of the algorithm and the measures provides a lot of information for the creation of new patterns as well as reinforcing those that are still useable".

On Zika and other demons

In a recent talk at the *Real Academia de Ciencias Exactas, Físicas y Naturales* (RAC), the virologist Esteban Domingo stated that: "A new viral infection appears every year; last year it was Ebola and this year it's Zika". This frenetic rate contrasts with the fact that it takes a decade to develop drugs to combat these diseases", says Elena Akhmatskaya, a researcher at the (BCAM - Basque Center for Applied Mathematics). A "faster and cheaper" alternative would be to model the virus in question, the organism it attacks and the chemical substance to be tested as an antidote. "After that, by means of computational techniques, thousands of hypotheses could be simulated in a matter of hours".

"So why are we still carrying out tests on animals and on volunteers?" asks Akhmatskaya. "Because no models exist that are complete enough to represent such complex systems, such as the human body or viruses", she replies, "and developing these models takes a lot of time. So far, it's been possible to reduce very simple viruses in plants to algorithms, but those that attack human beings are too complex".

While the search for antidotes goes on, epidemics continue to proliferate, and mathematics, as Antonio Gómez Corral explains, can provide "stochastic models that include the randomness of the real world for predicting with much greater precision the possible duration of the outbreak – flu this year, for example – and estimate probabilistically the number of individuals who may be affected over time". They may also enable foresee the medical protocols required in order to avoid a breakdown in health services.

At any rate, problems in biology are so many and so complex, says Akhmatskaya, that not only synergy with mathematics is necessary, but also with statistics, chemistry, physics and computation in order to develop sophisticated algorithms. "All is number," was Pythagoras' (570-495) dictum, and as Akhmatskaya concludes: "The more complex a problem is to solve, the more difficult it is to obtain the algorithms. And every little helps.

Tumor, don't resist!

Tomás Alarcón, a researcher at the Computational and Mathematical Biology Unit of the *Centre de Recerca Matemàtica* (CRM), explains that one of the main causes of the lack of effectiveness in cancer treatment is that cancerous cells develop a resistance to drugs. One of the "most suprising" results of his research work with mathematical models for tumor growth is that, "when the tumor is attacked with a particular drug, it behaves like an overexploited shoal of fish; those cells that best adapt to the new conditions, i.e., that chemical substance, are selected indirectly". If the same therapy is used over and over again, the tumor eventually becomes more resistant to it.

The ultimate aim is to establish as habitual in clinical practice the use of algorithms that include information about the patient and enable a personalized treatment, says Víctor Pérez, director of the *Laboratorio de Oncología Matemática* (MOLAB). This would provide a way of reducing the use of therapies that are not very effective.

Images of the cysts provide a great deal of data, and the challenge is to develop the appropriate models to predict the particular behavior the cancerous cells may have, based on real information, says Pérez, who concludes that: "At the moment, none exist that are being applied to assist in the decision-making process for patients suffering from cancer, but the outlook is promising".

ICMAT

Participants at Mathematical Perspectives in Biology workshop, held in ICMAT.

ICMAT

Ángela Capel en su despacho del ICMAT.

SHE MAKES MATH: Ángela Capel

ÁNGELA CAPEL

La Caixa- Severo Ochoa PhD student at the CSIC and member of the ICMAT

Field of Research: Quantum Information.

Problem she is working on: ¿When does a quantum system with many dissipative bodies have the property of rapid mixing?

Ángela Capel studies many-body quantum systems; that is, those formed by a large number of interacting particles. Specifically, she is interested in *dissipative* systems. Quantum dissipation finds its analogue in processes with irreversible loss of energy that arise in classical mechanics.

In the same way as when the temperature of a cup of hot coffee left on the table falls to room temperature, dissipative systems always converge to a stable state (in the case of the coffee, to ambient temperature) at a given moment, independently of their initial state. This stable state to which the system converges is known as the *fixed point* of the system, and the velocity of this convergence is measured according to the mixing time. *Rapid mixing* is said to take place when this velocity is high; that is, it grows logarithmically as the size of the system increases.

Capel's PhD thesis, supervised by David Pérez García (UCM-ICMAT), seeks to characterize rapid mixing. In the classical world this property is the equivalent of other important problems in physics, such as the existence of the spectral gap. The aim is to determine whether these equivalences also appear in the quantum world. To that end, Capel employs tools belonging to functional analysis, matrix analysis, convexity and even geometric intuition.

You can find an extended version of this profile on the blog "Mujeres Con Ciencia".

IDEAS FOR POST-QUANTUM CRYPTOGRAPHY

"Elliptic curve cryptography is not the long-term solution we hoped it would be. That's why we are obliged to rethink our strategy". With these words, the USA National Security Agency (NSA) warned some weeks ago about the need to find new cryptogaphic tools in order to ensure the security of communications across the Internet. In a communiqué on its website, the Agency expressed its interest in "initiating a transition to quantum resistant algorithms in the not too distant future". It regards the development of such security tools against a potential quantum computer as a prime objective. One of the ideas in the so-called post-quantum-cryptography is multivariate cryptography. Ignacio Luengo (UCM-ICMAT) and Jorge Linde (CSIC-ICMAT) are currently developing new techniques in this field.

Ignacio Luengo and Jorge Linde. In recent decades, the Internet has attained a prominent role in society. One of the principal mainstays on which the Net is based is Public-key Cryptography, which among other things enables private communications, the identification of users in a server and the signing of documents to be carried out safely. Among the different methods employed for this public-key encryption is the RSA algorithm, which is based on the factoring of very large prime numbers. However, already in 1994 Peter Shor presented an algorithm that enables large prime numbers to be factored, and thus is capable of bringing the entire system down.

The only reason why Shor's algorithm has not so far jeopardized the security of the Internet is that it can only function in a quantum computer, which would work with thousands of Qubits. No such computer exists at the present time, but current advances in quantum computing suggest that a quantum computer with these features could be built within a few decades. It is therefore necessary to tackle this prospect as soon as possible. The main worry at present is *backward in time security*; that is, as if everything we are encrypting now could be decrypted in a few decades when the quantum computer has been built.

At the last congress on Post-Quantum Cryptography, the PQCrypto 2016, the National Institute of Standards and Technology (USA) warned how urgent it is in the next few years to find and standardize a cryptographic system able to withstand the Shor algorithm in order for the Internet to remain as we know it should the quantum computer be built.

Post-quantum cryptography is the field of study for these types of cryptographic systems that are not affected by quantum computers. One of the techniques employed is *multivariate cryptography*, in which systems whose difficulty resides in the complexity of solving systems of polynomial equations in many variables.

Despite the advances made in this field, there is at present no multivariate system that is safe and efficient. The work on which we are engaged, and to which Jorge Linde's doctoral thesis belongs, is aimed at developing by new techniques a multivariate system that could be one of those chosen by the NIST for standarization.

Ignacio Luengo is a professor with the Faculty of Mathematics Department of Algebra at the Complutense University of Madrid and a member of the ICMAT. Cryptography, algebraic singularities and motivic integration are among his current research interests.

Jorge Linde is on a Severo Ochoa FPI contract at the CSIC and a member of the ICMAT. He began his doctoral thesis on multivariate cryptography in December, 2014, and is supervised by Ignacio Luengo.

N. Gregory Alamy

INTERVIEW: Kenneth Chang

"It's very complicated to write about new results in mathematical research"

100xCiencia

Ágata Timón G. Longoria. Kenneth Chang says that he would never have made a good physicist. So after a few years he dropped his doctorate studies to devote himself to something he never imagined would become his profession – writing about science. He has been doing this for the last fifteen years at The New York Times, regarded as perhaps the best newspaper in the world. Some 20 people work on the science section in this paper, which is the touchstone for all other science editors. It is for this reason that he was charged with giving the inaugural address at the *I Foro 100xciencia*, which last October on the island of La Palma brought together science journalists and representatives belonging to the Spanish Severo Ochoa research centers. It was there where we had the opportunity to talk to him about his experience with mathematics as a science journalist.

Q: How would you describe how mathematics is presented in the Science Section of The New York Times in comparison with other scientific disciplines?

A: There's very little difference. The mathematics one learns at school appears occasionally in items on mathematical education, and basic mathematics is also used for analyzing surveys and things like that. But it's very complicated to write about new results in mathematical research and make them accessible for people. There are some exceptions: Kepler's conjecture is something everyone can understand because it's about how oranges are stacked.

Q: From time to time you write about mathematics, don't you?

A: Well, it's something I'd like to write more about, but it's difficult and requires a lot of effort to understand what one is supposed to talk about. It's hard to evaluate an advance in mathematics; what's important about it, what's new... What's more, you need a "hook", some way of explaining the result to the general public beyond just saying that "a difficult problem has been solved".

Q: What kind of articles appear in The New York Times about mathematical research?

A: What we publish most are obituaries about mathematicians. Just like any other person, you can draw a profile of a mathematician, and that's where some information about his or her research work often appears. We always cover the Fields Medals, but basically we give the names of the prize-winners and include a few lines about why they have been awarded the prize. We don't say too much about the research work, but I have to say that we don't receive any information from the institutions to which the prize-winners belong. On the other hand, obviously if an important conjecture has been solved it qualifies as news.

Q: Do you remember any important news story concerning mathematical research?

A: The last big story was about Perelman's resolution of the Poincaré conjecture. Perelman was a great character; he embodied the stereotype of the oddball, solitary mathematician. This type of item works, but it's still a stereotype. When Terence Tao won the Fields medal I wrote a profile of him and was able to talk to him. He was a child prodigy and he's made some impressive achievements, but he seems to be an amazingly normal person.

Q: In general, what's your experience of working with mathematicians been like?

A: One mathematician told me that there are three kinds of mathematicians: the type who only talks about mathematics; the type who, in spite of being able to talk about other things, hasn't enough English and so only talks to others in the first group, and finally those who do talk about other things. The nature of mathematical research is that enables the loners to go to their offices and do their own thing without bothering about anything else, so it's the kind of profession that attracts people with this profile. But there are other types as well. The loners don't want to talk to journalists, they just want to do math, but the others are excited about sharing what they find fascinating about mathematics.

Q: How do you find out about the latest developments in mathematical research?

A: People usually send me information. Some of the emails don't make much sense, but if I receive the same news from several people, I start to pay attention. Also my brother is a mathematician and he usually lets me know when something important happens.

Q: Have you any advice for the mathematical community about how to improve the way they communicate?

A: It's always necessary to try and give the big picture. Otherwise, if you only say that some obscure lemma has been solved, it's not going to interest anybody. What's more – and I know mathematicians hate doing it – you have to talk about the applications of a result in order to give people an idea of the what you're talking about. It's vital to find a way of explaining a problem in terms that the general public can understand.

SCIENTIFIC REVIEW: A participatory budget model under uncertainty

Title of article: A participatory budget model under uncertainty.

Authors: J. Gómez (Real Academia), D. Rios Insua (Instituto de Ciencias Matemáticas), C. Alfaro (Real Academia).

Source: European Journal of Operational Research. Volume 249, Issue 1. Pages 351–358.

Date of publication: February 16th, 2016.

doi: 10.1016/j.ejor.2015.09.024

More than 1,500 municipalities throughout the world have set up a scheme known as *Participatory Budgets.* The idea is based on enabling citizens to decide directly on what a part (or all) of available public money should be spent. These experiences usually arise from the response to the demand in local government and municipal authorities for greater citizen participation in public policies.

The issue at stake is that of decision-making by a group, and the aim is to develop models and methodologies for facilitating this process by using available information and promoting transparency and consensus. The models under consideration so far assume a fixed budget based on the maximum amount of money that can be spent. However, in crisis situations where public funds may suffer unexpected cuts, such an approach may not be the most appropriate. In the private business sector, flexible budgets are employed that are better adapted to factors of uncertainty.

David Ríos, director of the AXA Chair at the ICMAT, together with researchers from the Royal Spanish Academy of Sciences, Javier Gómez and César Alfaro, have published a paper in the European Journal of Operational Research on a methodology for the drawing up of participatory budgets in conditions of uncertainty on the basis of stochastic programming and the extension of decision-making by groups based on voting, negotiation and arbitration in the case of uncertainty.

Participatory budgets can be considered as an issue in which it is necessary to distribute a limited number of resources among a set of projects with the aim of maximizing some sense of participant satisfaction while fulfilling certain restrictions. The amounts under consideration, such as the costs of a project or the budget available, may be subject to uncertainty. In their work, these researchers incorporate flexibility into the classical problem of participatory budgets so they can be adapted to economic and financial contexts of uncertainty.

Uncertainty appears in the estimated cost of different projects, in the total available budget and the valuation of the projects (which is calculated by both municipal appointees and citizens themselves). The distribution of the budget has to fulfil certain conditions, among which it is necessary for the total amount of the costs established for each project to be less than the budget in total. Further restrictions may be added, such as that the cost associated with certain types of projects should not exceed a certain percentage of the total, or that various similar projects should be mutually excluded, or, on the other hand, that various dependent projects should exist (and if a budget is assigned to one, it should include the other).

In this way, a more flexible and realistic budget can be drawn up that is also adaptable to different styles of decision-making as well as a more effective use of the information provided by participants. This methodology could be used as a profitable alternative to the more rigid and unsoundly-based methodologies that prevail in the majority of municipalities where they have been put into practice. A recent example that may be cited in this regard is the city of Madrid, where a rather simplistic approach has been adopted.

David Ríos (Madrid, 1964) is the director of the AXA-CSIC Chair of Adversarial Risk at the ICMAT. A full member of the Spanish Royal Academy of Exact, Physical and Natural Sciences, Ríos gained his degree in Mathematical Sciences from the Complutense University of Madrid (Extraordinary Prize, National Prize) and his PhD in Computation at the University of Leeds. His current research work is focused on the fields of Decision Analysis, Negotiation Analysis, Bayesian Statistics and Risk Analysis and their applications to the protection of critical infrastructures, social robotics and electronic participation, among others. His approach to research is based on real complex problems in decision-making, which lead him to methodological innovation and which often become new systems that help in the decision-making process.

Javier Gómez (Madrid, 1982) is a Computer Science Engineer. He holds a Doctorate in Computer Science and a Master in Decision Making Engineering from the URJC. He currently works at the Real Academia de Ciencias (RAC – Royal Academy of Science) as a researcher and is engaged in the "Methodology for Risk Management in Operational Flight Security at a State Level" project, which is undertaken in collaboration with the AESA. His research work is focused in Big Data Analysis and the development of tools applied to different fields, such as social innovation, risk analysis, operation security and sensitivity analysis.

César Alfaro (Madrid, 1982) is a Computer Science Engineer. He holds a Master in Decision Making Engineering and a Doctorate in Information Technology and Computer Systems from the URJC. He is currently a researcher at the RAC where he works on problems concerning air safety. His research work is focused electronic participation, the development of tools for sensitivity analysis and opinion mining as well as risk analysis and its applications.

"Being a researcher increases one's capacity to explain complex things"

MIGUEL DOMÍNGUEZ VÁZQUEZ

Miguel Domínguez Vázquez was born in Grou (Ourense) in 1985. A female mathematics teacher he had when doing his baccalaureate taught him the importance of rigour. Following this idea, he decided to take a degree in Mathematics at the University of Santiago de Compostela, where he also gained his doctorate in 2013. He subsequently went on to do various post-doctoral stays, first at Kings College, London, and later at the National Institute for Pure and Applied Mathematics (IMPA, Rio de Janeiro, Brazil), where he worked for two years. Since January, 2016, he has been a Juan de la Cierva post-doctoral researcher at the ICMAT under the supervision of Alberto Enciso. His wish is eventually to return to Galicia, the country of his birth, to teach mathematics and continue his research work there.

Francisco Gozzi

Elvira del Pozo Campos. When Einstein presented his Theory of Relativity, a journalist asked him if he could explain it in a simple way, to which Einstein replied: "Could you tell me how to fry an egg?" The journalist frowned and nodded his head, and then Einstein added: "Do it, but imagine that I don't know what an egg is, or a frying pan, or cooking oil, nor even fire". In this graphic way, Einstein, who was also the father of gravitational waves, draw attention to an important fact: that it is complicated to communicate abstract ideas.

This is also how Miguel Domínguez feels about the matter. For him, it is all about a "philosophical problem" that is difficult to solve, despite that fact that "being a researcher increases one's capacity to explain complex things". In his opinion, it is not only desirable but also "necessary" to convey to people what the geometric and topological problems he works on are really about, as well is stressing their importance and the need to devote public money to progress in these fields.

"It is not only desirable but also "necessary" to convey to people what the geometric and topological problems he works on are really about, as well is stressing their importance and the need to devote public money to progress in these fields"

Miguel works on Riemann geometry in which space is curved. This brings us back to Einstein again; this idea mathematically underpins General Relativity. In the end, this is essentially a geometric theory of gravity in a universe of four dimensions that undulates due to the presence of matter and radiation.

As Miguel explains, the XIX century German mathematician, Bernhard Riemann, established a theoretical framework suitable for the study of a broad range of geometries by means of tools belonging to analysis. His contribution consisted in the development of a single "complete mathematical theory encompassing the elementary laws for individual points to the processes that appear before us in space continuously full of reality, without distinction between gravitation, electricity, magnetism or thermostatics," as stated by Riemann himself at the age of 24. Thus, Euclidian and non-Euclidian Geometry are particular cases of Riemann geometry.

Miguel is engaged on the so-called *isoparametric submanifolds*, a type of "highly symmterical" subspaces that appear in Riemann's theory. "If a space of multiple dimensions were a room, I would study the surface of a ball or a float inside the room," explains this researcher. This field falls within the line of research initiated by the French mathematician Élie Cartan (1869-1951) in the early XX century. It is an area in which tools belonging to Riemann geometry and to Lie groups (which "formalize the intuitive idea of what a symmetrical object is") come together. It also employs differential equations, topology and conmutative algebra.

First cousins

One of the works of which he is most proud is the one that led him to the discovery of a "very nice and surprising" relation between prime numbers and submanifolds with a high degree of symmetry. He says that, to date, "no links were known between the area of Riemann geometry and prime numbers".

Miguel often repeats the word "nice" when talking about research. His passion for research work is especially motivated by the artistic facet that is implicit in mathematics. He likes to think that "mathematicians uncover a reality that was always present but remained unknown, and the art resides in doing so by means of the most simple, profound and elegant deduction".

"Mathematicians uncover a reality that was always present but remained unknown, and the art resides in doing so by means of the most simple, profound and elegant deduction"

"Like Michelangelo, who envisioned David in the unhewn stone and revealed him to the world in the most beautiful way", he adds. And like Einstein, who imagined a geometric space and thereby predicted the existence of black holes and gravitational waves. He goes on to say that: "In the future, I'd like someone to find applications to my field of research", something which at the moment he is unable to imagine. However, until then his goal is to contribute to further advances in knowledge and to improve teaching in this field of mathematics, which in itself is no small accomplishment.

MATHEMATICS TODAY

ANDREW WILES AWARDED THE ABEL PRIZE FOR HIS PROOF OF FERMAT'S LAST THEOREM

The 2016 Abel Prize was awarded on March 15th of this year to the English mathematician Andrew Wiles for his proof of Fermat's Last Theorem. The prize is worth 600,000 euros and will be presented to Wiles on May 25th by Crown Prince Haakon Magnus.

On March 15th, the Norwegian Academy of Science and Letters announced that the 2016 Abel Prize would be awarded to 62 year-old Sir Andrew J. Wiles, "for his stunning proof of Fermat's Last Theorem by way of the modularity conjecture for semistable elliptic curves, opening a new era in number theory". Fermat's Last Theorem presents a simple relation of integers. It states that when n is greater than 2, there are no positive integers x, y and z that satisfy the equation $x^n + y^n = z^n$.

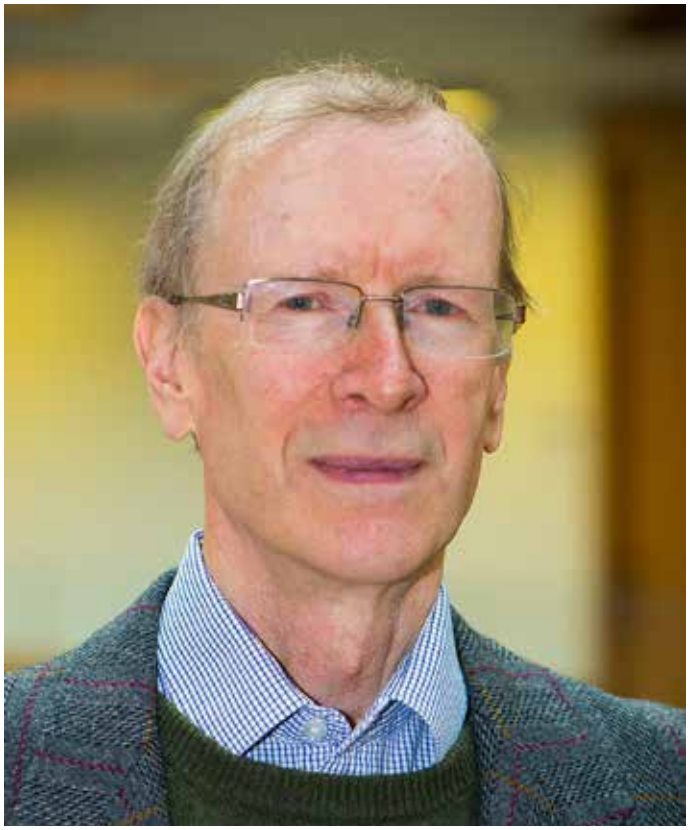
In the words of ICMAT director Antonio Córdoba, who in 1994 had the occasion to celebrate the solution with Wiles at Princeton University: "Andrew Wiles scaled the heights of one the most coveted achievements in mathematics, both for its historical significance and its importance in the development of the discipline. His work brought to an end the search started by Fermat three and a half centuries ago and in which other mathematicians such as André Weil, Goro Shimura and Yutaka Taniyama have also played a decisive part".

The Weil-Shimura-Taniyama conjecture is the result of work by these three mathematicians and which concerns modular forms, an area of mathematics that in principle has no relation with Fermat's Theorem. Nevertheless, mathematicians Kenneth Ribet and Gerhard Frey observed a connection between both problems. "That's where Wiles' adventure began in solving a problem that had intrigued him since childhood", says Córdoba. Wiles first came across Fermat's Last Theorem when he was ten years old. As he declared in the Norwegian Academy of Science communiqué, "I know from that moment I would never let it go. I had to solve it".

That is why he devoted eight years, in complete isolation, so it is said, to the proof of a special case of the Weil-Shimura-Taniyama conjecture, on the basis of which he deduced Farmat's Last Theorem. The first proof he announced in 1993 turned out to contain an error, but after a further two years of intensive work in conjunction with Richard Taylor he managed to correct it. He presented the complete solution to the problem in 1994.

The Abel Prize Committee stated that; "few results have as rich a mathematical history and as dramatic a proof as Fermat's Last Theorem". According to the Committee, "it was the most famous unsolved problem in the history of this branch of mathematics".

The story of this result began three centuries ago when the French mathematician, Pierre Fermat, posed the problem after reading an edition of Diophantus of Alexandria's *Arithmetica* in which he deals with Pythagoras' Theorem. Fermat subsequently wrote that; "I have discovered a wonderful proof of this statement, but the margin is too narrow to contain it". However, the proof did not turn out to be as straightforward as Fermat first suggested. As Antonio Córdoba says; "the problem is especially important because of the large volume of mathematics that have arisen from its solution: the theory of ideal numbers, the study of algebraic bodies, and so on".



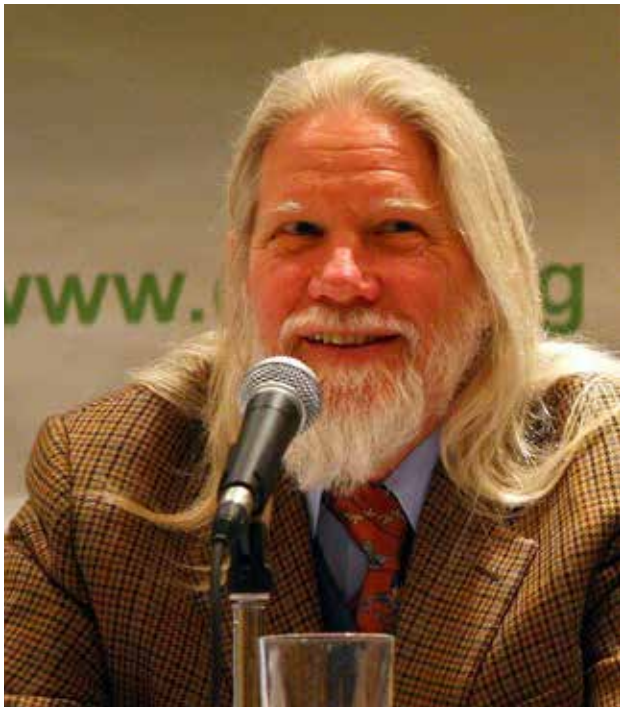
Alain Goriely/University of Oxford

Andrew Wiles

The award of this prize at last signifies the deserved recognition of a mathematician who once narrowly failed to qualify for a Fields Medal. When he presented his first proof of the theorem he was not quite 40 years old, the age limit fixed for the candidates for this prize. However, in the two years it took him to arrive at the correct result, he passed the age of forty and thus was not eligible for the award. In 1998 he received a silver Fields Medal (the IMU Silver Plaque, the only time that such a distinction has been awarded) as a special tribute, and now in 2016 he has been honoured with the Abel Prize.

THE 'NOBEL PRIZE OF COMPUTING' GOES TO THE FATHERS OF SECURE COMMUNICATION ON THE INTERNET

Simon Law (de wikipedia)



Whitfield Diffie

Alexander Sigachov (de wikipedia)

Martin E. Hellman

The encryption of emails and online transactions are mainly based on the asymetric cryptosystem and electronic signature devised by Whitfield Diffie and Martin E. Hellman (USA) at the height of the cold war. They have been recognized with the Turing Award 2016 by the Association for Computing Machinery (ACM) for their "decisive contribution to modern cryptography", which enables secure communication for users, banks, businesses, servers and the cloud across the internet.

The award is regarded as the Nobel Prize for Computing and refers to a crucial moment in 1976 when the two winners, the current head of Sun Microsystems and this professor at Stanford Univesity, respectively, published an article entitled New Directions in Cryptography. In this article they announced a new cryptographic algorithm known as the Public Key, which was subsequently given the name of its discoverers, Diffie-Hellman, and with which they would contribute "to a future when people would communicate with each other regularly through electronic networks. This would make their communications vulnerable to theft or interference," says Alexander L. Wolf, president of the ACM. Now, forty years later, he goes on to say, their foresight proved to be "extraordinarily" prescient.

In cryptography, a key is a code used to transform a legible text into another that is incomprehensible, and vice-versa. In the two-key cryptographic system devised by the award-winners, a public code, which is not secret and can be freely distributed, is used to encrypt the message, while another private code, which is known only to the receiver, is used to decrypt it. The first code locks the content of the communication and the second is the only key that can open it. If applied the other way round, the digital signature is used. The sender of a message uses a private key to sign the content, while the receiver uses the sender's public key to verify the digital signature. It is as if an envelope were stamped with an unmistakable seal and could be authenticated by anyone who opened it.

The award is endowed with one million dollars (approximately 887,000 euros) and bears the name of Alan Turing, the British mathematician and cryptographer who deciphered the Enigma machine, used by the German military for sending messages during World War II. At that time, the systems were symmetric (sender and recever used the same key), and this required a secure channel for transmitting the key, which was not always easy to achieve. On the contrary, if the same code was used too often, it could provide enough enciphered text for the Allies to decrypt it. Perhaps if the Diffie-Hellman system had existed then, Turing might not have solved the *enigma*.

MATHEMATICS TODAY

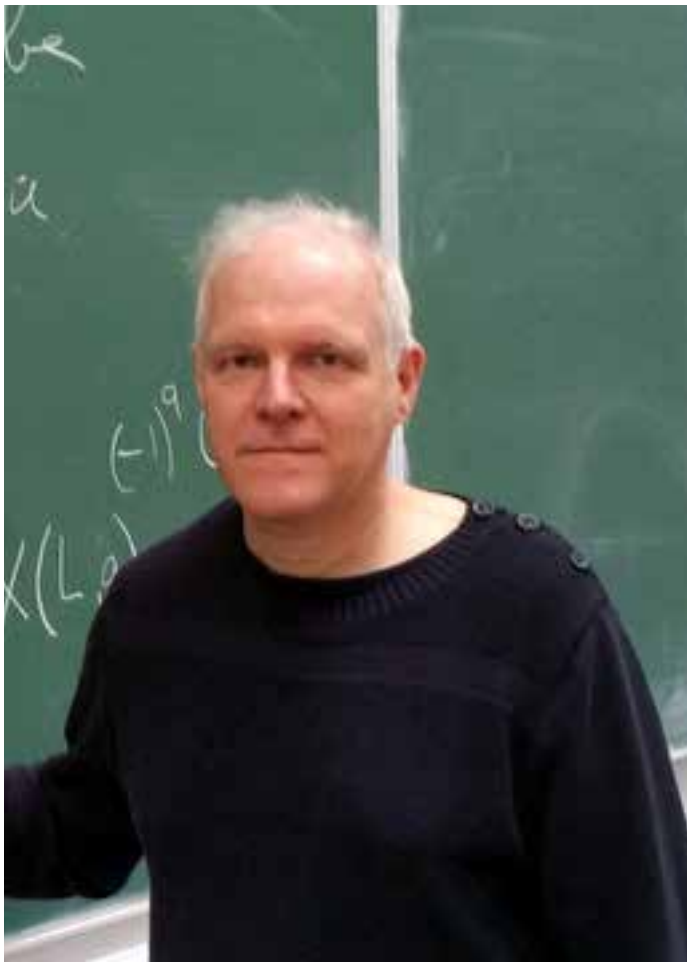
Pioneers in Geometry and Complex Analysis

ERIC BEDFORD AND JEAN-PIERRE DEMAILLY AWARDED THE STEFAN BERGMAN PRIZE

AMS

Eric Bedford

AMS



Jean-Pierre Demailly

In March of this year, the American Mathematical Society (AMS) announced the winners of the 2015 Stefan Bergman Prize. They are Eric Bedford and Jean-Pierre Demailly. This prize is worth 12,231 dollars (approximately 10,500 euros) and is awarded in recognition of the pioneering work that these two mathematicians have conducted in the fields of complex aalysis and complex geometry, both of which are "fundamental for mathematics" says Duong Phong, the chair of the selection committee.

Phong explained that the work carried out by Bedford and Demailly "has had, and continues to have, and enormous influence, especially in the fields of complex differential geometry and the theory of Monge-Ampère equations". In particular, Eric Bedford is known for his contributions to the theory of several complex variables and complex dynamics, as is Demailly, who is regarded is one of its most influential figures.

Introduced in 1988, the prize honors the memory of Stefan Bergman, one of the most highly recognized researchers in the field of complex variables. Bergamn lent his name to the Bergman projection and the Bergman kernel function. Although born in Poland, he taught at Stanford University for many years. After his death, his wife stipulated in her will that funds should be devoted to a prize awarded in memory of her husband.

ICMAT News

THE ICMAT RECEIVES THE SEVERO OCHOA CENTER OF EXCELLENCE ACCREDITATION

MINECO

Carmen Vela, Spanish Secretary of State for Research, Development and Innovation, with the representatives of the SO Centers which obtained their distinction in 2015..

On February 2nd of this year, Carmen Vela, the Secretary of State for Research, Development and Innovation, presented the Severo Ochoa accreditations of Excellence to those centers who obtained them last October. Among the research centers to receive this distinction was the Instituto de Ciencias Matemáticas (ICMAT), which was distinguished with this award for the second time running.

The accreditation is valid for a period of four years and is endowed with a total funding of four million euros. Says Diego Córdoba, ICMAT member and the principal researcher for the Severo Ochoa project: "This is a further confirmation of the international standing of the ICMAT. The Institute aspires to be among the very best research centers in the world, and thanks to the renewal of the Severo Ochoa program this ambitious project can be consolidated".

"The Severo Ochoa project is vital for the ICMAT to be able to tackle the program of activities that have made it a home for the international mathematical community and the driving force for the development of mathematics in Spain", states Antonio Córdoba, recently appointed as director of the ICMAT. In his opinion, "obtaining this new accreditation for the period 2016-19, and thereby confirming the recognition already obtained for the 2012-2015 period, means the consolidation of the ICMAT project and a great stimulus for the future". Together with other sources of funding from the European Community, from the MINECO, and entities such as LA CAIXA, BBVA and FUJITSU, this funding from the Severo Ochoa constitutes the main resource, says Córdoba.

This distinction is granted to research centers that have a strong scientific impact and leadership internationally and which are regarded as the best in the world in their respective areas. Each institute receives a million euros annually to help to improve research of excellence in each different field.

30 SECONDARY-SCHOOL STUDENTS EXPERIENCE MATHEMATICAL RESEARCH FIRST-HAND AT THE ICMAT

Over a period of three days the ICMAT hosted 30 pupils from 25 secondary schools in the Community of Madrid in order to show them how mathematical researchers work at a center of excellence. Mathematics concerning the theory of relativity and the grand unified theory, graph theory and algebraic congruencies, and a career in mathematical research are just some of the subjects presented in the program. This initiative forms part of the Community of Madrid "4ESO+empresa" scheme that enables students to do stays and visits at companies and research centers.

For the fourth consecutive year, the ICMAT participated in the "4ESO+empresa" scheme with 25 schools from the Community of Madrid. On the 15th, 16th and 17th of March, 30 4th Grade secondary-school students worked alongside scientists from the center as part of a program whose aim is to enable pupils to experience the daily work of a mathematician for themselves.

ICMAT

The main aim of the activities was to bring the students into direct contact with a type of mathematics different from that they learn in the classroom, one that is creative, exciting and related to other branches of knowledge. To that end, the program included activities conducted by young researchers belonging to the center. "They are the protagonists of these activities because they provide the closest model for the students", says Manuel de León, who is responsible for this initiative at the ICMAT. David Alfaya, a La Caixa-Severo Ochoa PhD student, organized a mathematical competition in which the students, divided into groups, had to tackle various mathematical challenges. Ángela Capel, who is also a La Caixa-Severo Ochoa doctoral student, and María Ángeles Ferrero, an FPI-Severo Ochoa PhD student, gave talks in their workshops on modular arithmetic.

In addition to these workshops, a talk was also given by Marie-Curie post-doctoral researcher at the ICMAT, Mario García, on the relation of mathematics, specifically geometry, to the most up-to-date physics; the theory of relativity and the grand unified theory; a session of creative and exciting mathematical problems conducted by Marco Castrillón (UCM-ICMAT), a talk about the ICMAT and mathematical research as a profession, given by Manuel de León (CSIC-ICMAT), and a workshop run by Florentino Borondo (ICMAT-UAM). ICMAT director Antonio Córdoba welcomed the students, while Ricardo Martínez de Madariaga, head of the CFTMAT Library, introduced the students to the library facilities.

THE ICMAT COLLABORATES FOR THE FIRST TIME IN THE CÍRCULO DE BELLAS ARTES SCIENTIFIC FAIR

ICMAT

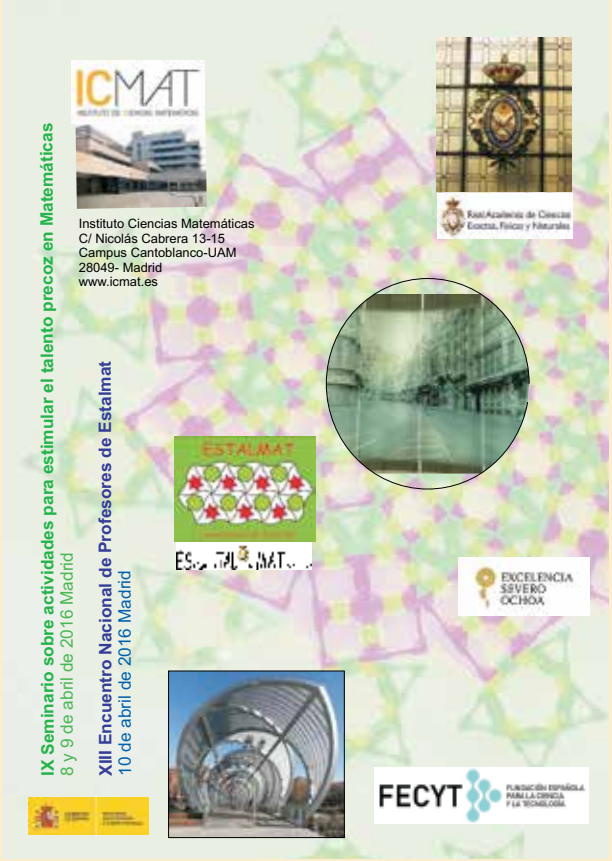
María Barbero (UPM-ICMAT) was the director of the workshop "¿Vivimos en un mundo áureso?".

The Universidad Politécnica de Madrid professor and member of the ICMAT, María Barbero, conducted a total of four sessions in the "Do we live in a golden world?" workshop as part of the Círculo de Bellas Artes "With Science in Schools" program. This activity, which was held on March 9th and 10th, enabled pupils from Madrid to show their scientific projects to the general public and to students from other schools, as well as to enjoy the outreach activities that were organized in parallel.

The Golden Ratio and the Fibonacci sequence were the main mathematical features of the "Do we live in a golden world?" workshop given by María Barbero, professor at the Universidad Politécnica de Madrid and ICMAT member on March 9th-10th. The activity formed part of the Círculo de Bellas Artes "With Science in Schools" scientific fair, in which the ICMAT collaborated this year for the first time.

After an introduction of a theoretical nature, the students were able to experiment with ideas in mathematics. They looked for the Golden Ratio in books, sheets of paper, in ID documents and in their own faces with a ruler and compass they fashioned themselves. Finally, they had to come up with the winning strategy for a simple board game by experimenting, conjecturing and seeking a general answer to the problem. And lo and behold, the Golden Ratio appeared in the solution.

AGENDA



ICMAT
INSTITUTO DE CIENCIAS MATEMÁTICAS

Quarterly Newsletter
Instituto de Ciencias Matemáticas
#12 I Quarter 2016

Production:
Instituto de Ciencias Matemáticas (ICMAT)
C/ Nicolás Carrera nº 13-15
Campus de Cantoblanco, UAM
29049 Madrid ESPAÑA

Divulga S.L
C/ Diana 16-1º C
28022 Madrid

Editorial Committee:
Manuel de León
Ágata Timón
Kurusch Ebrahimi Fard

Coordination:
Ignacio F. Bayo
Ágata Timón

Design:
Fábrica de Chocolate

Layout:
Equipo globalCOMUNICA

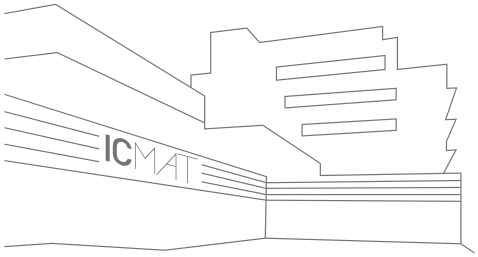
Translation:
Jeff Palmer

Editorial department:
Elvira del Pozo
Ágata Timón

Creative Commons
CC BY SA

ICMAT

INSTITUTO DE CIENCIAS MATEMÁTICAS



C/ Nicolás Cabrera, nº 13-15
Campus Cantoblanco UAM
28049 Madrid, Spain
www.icmat.es

ICMAT
GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD
CSIC
UAM UNIVERSIDAD AUTÓNOMA DE MADRID
excelencia UAM CSIC
EXCELENCIA SEVERO OCHOA
UNIVERSIDAD COMPLUTENSE MADRID