Interview with Preda Mihăilescu

Göttingen (Germany)

from left to right: Samuel J. Patterson, Preda V. Mihăilescu, Axel Munk and Hanno Ehrler

***Preda V. Mihăilescu**, born in Bucharest, Romania, is best known for his proof of Catalan's conjecture. After leaving Romania in 1973, he settled in Switzerland. He studied mathematics and informatics in Zürich and then pursued a career as a mathematician in the Swiss banking sector. While still working in industry, he received his PhD from ETH Zürich in 1997. His thesis, titled Cyclotomy of rings and primality testing, was written under the direction of Erwin Engeler and Hendrik Lenstra.*

Mihăilescu started to work in academia as a research professor at the University of Paderborn, Germany. Since 2005 he has been a professor at the Georg-August University of Göttingen (Germany).

This interview took place on 3 December 2007 at the Mathematisches Institut of the University of Göttingen. It was prepared by Axel Munk (Mu) and Samuel Patterson (Pa), both from the University of Göttingen, who also participated; it was conducted by Hanno Ehrler from Deutschlandfunk, a German public broadcasting channel.

Childhood and education, Romania and Switzerland

First of all, I would like to ask you to tell us a little about your curriculum vitae, starting with your childhood. I read in an article that you had a talent for mathematics and numbers very early on.

The game with numbers indeed started about the age of four, and before I was five I had the reputation of the child who multiplies three digit numbers. I liked the game and could not understand what others found so astonishing about it – a little bit like listening to music that not many appear to notice. There were variations; friends of the family who were engineers visited and verified my 237×523, say, with a slide rule – and I found it quite awkward when I looked at "the competition". I saw all these lines at varying distances on the slide ruler and realized that it could never yield the precise 6 digits of the result, since the maximum accuracy was 5 digits. So I knew that the verification was only approximate – yet I knew that my result was precise. It was different on the playground; only much later did I learn that the older people whom I did not know and who came making their challenges – sometimes they even tried to teach me to perform multiplications on paper – had actually made bets with their friends.

Of course this gave a predisposition for mathematics, but it was not cultivated in any particular way for quite a while. Humanities came first in my early life.

What other important recollections do you have from your childhood?

My childhood was relatively protected at a time of intense dictatorship. My parents did not hide from us all of what was happening. Thus we knew that an uncle was in a camp and that others had no job or worked as street dog catchers (it happened), having been poets and philosophers before that. We knew that twice a year my grandfather visited his former professor and master, who had recently finished his camp sentence, taking him a large dried sausage, which made the old man cry. Then they had several hours of discussions, which brought them back into the spiritual fields of their youth; I sensed a particular intensity in my grandfather when he was coming back from these visits, like a veil was raised for a brief period of time over a world I would never encounter in my own life.

We knew that we had to be careful about what we said and we feared the power – but in fact I had little direct contact with "those guys" as a child. The parades, the songs and the doctrines were visible but not so tangible as the family circle that was offering comfort. Eventually, when going to school, a third category emerged: the school teachers, some of whom were really nice – yet they were employed by "them" so one could not be sure. For us, Stalinization came to an end towards the mid-60s, although it formally ended in 1956. In the 60s there was, on the one hand, an amnesty and many people came out of camps, and on the other hand ... there was "Strawberry fields" and "Penny Lane". If I recall correctly, we heard the first Beatles songs even on public radio. By the time I was able to consciously ask the question: 'why did one grandfather die under untold conditions while the other one lives with us to the greater joy of all, why did uncles disappear, and whether or not we had been close to such a destiny?' a sort of a warmer wind was blowing.

And then, when I became a teenager I was elected, as a good pupil, to some leading communist youth role in the school. I thought I was choosing a smart way out by basically saying at the meetings that one should try to be oneself even within this organization because according to what they said, they actually expected this from the youth – and not, like everybody knew, frightful obedience and indoctrination. The words were not exactly these but the meaning was quite clear, and after several

calls to order in offices of higher ranking "comrades", I came to understand that I did not have all one needs for civil disobedience. This may be one of the personal experiences that made me choose, four years later, to seek asylum in Switzerland.

And there you studied mathematics?

And there I studied mathematics and entered a new life that was challenging in all directions.

There were two things that led me to the choice of doing applied mathematics: one was the pragmatic estimate of survival odds for the inexperienced refugee that I was. But this could never suffice, not without the feeling of being in a world where one could do things, a lack of limitations that had to be experienced. So I went to do something that none of the males of my family had done, at least in the last three generations – become practical. They had all ended up teaching in one way or another; I was going to work in some productive area – quite ironic, looking back now, isn't it? It is probably from my mother that I have learned a love for very practical, well done things. She was a gynaecologist and a surgeon. Delivering babies under the most difficult conditions, both medical and physical, was an unspoken, penetrating passion for her. From her I think I received the love for things with a practical purpose – developing a project like delivering a child, bringing something new to life...

Industrial career

So it is quite natural that you studied applied mathematics and then went into industry. What did you do there? What kind of work did you have to do?

There are two periods of my industrial career. After the second "Vordiplom" in mathematics until the end of my computer science Masters degree, I worked, with interruptions, in a company in the machine industry. I applied numerical analysis and developed methods and programs for designing models of turbine blades so that the gas flow around these blades could be computed exactly. It is a typical application meant to provide reference data for testing larger software packages. From the desire for a visual interaction with these models, I was led to several visualisation applications; in the end, I even developed a visual interface for software that computes load flow and short-cut simulations in large electrical networks. It was an effective sales argument for that specialized, professional software and my first application that had an impact on the market. That was also in the very early beginnings of graphical interfaces so I had to invent many of the tools I needed pretty much from scratch.

Then, after completing my computer science studies, I switched to information security. I worked in that domain first in banks and later in a consulting and development company. I would say that in the productive phases of my industry life, I was peacefully conceiving projects and bringing them to life, and there was nothing spectacular about it. The security of online ATM system in Switzerland, for example, which has been running since 1990 with some natural renewals and no essential changes to the core, has withstood the test of time and represents the silent success behind that work.

What does "information security" mean? Were you concerned with security systems?

Yes – security of information. That means protecting data on the net against intrusion or modification, protecting identities – in the sense that the identity of a person may be associated with documents or "electronic signatures" in an inalterable and irrevocable way – and variations of these basic problems of confidentiality and identity. The methods used belong to the field of cryptography, which uses number theory, and this is why a mathematician was preferred. The mathematical background was certainly useful so that the cryptographic issues were easily accessible. From my point of view – and probably not only mine – the challenge of the job was to supervise a large system so that no security gaps arose. Gaps due to organizational reasons rather than purely cryptographic ones often played the most important role; cryptography is well under control due to the theory.

It was also the beginning of public key cryptography and I had a lot to do helping potential users be a bit more sensible. Primarily, security made the life of the normal programmer or computer user slightly harder, not only because of the numerous password protected applications one had to sign into sometimes dozens of times a day but also because a secured application could, at that time, be logically slower. One had to convince co-workers to accept such inconveniences to enforce the security of the internal network.

At one stage, I was employed in the most important bank in Switzerland, which had the ambition of being ahead of its time in IT; it could also afford to pursue this goal. At that time the term "single sign-on" was starting to be coined as a desirable alternative to the multiple applications asking for a password on the desk of every employee. The technology answering the expectations of this time was only developed over five years later.

I was asked if I "could develop a single sign-on system" for the company's network. What I was doing practically at that time was cryptographically securing the communications in the bank. This was very useful and could be done with the manpower available. I was unsuccessful in using a detailed technical argument to explain that "single sign-on" was not at that time within reach. On that occasion, I learned that sometimes a negative proof is not accepted as a basis for a decision. Maybe that experience made me wish for an environment where a negative proof is well regarded; anyhow, years later I was able to present a negative proof, which confirmed Catalan's conjecture, and that one was very well accepted.

Pure mathematics during spare time...

So we are back to pure mathematics. As I know, you also had time for studying pure mathematics; after all, you solved Catalan's conjecture. How was it possible to

have this job in the bank and the work in industry and at the same time be concerned with pure mathematics? Is it some kind of hobby or an inner drive?
The inner drive was there and mathematics was also helpful for my mental balance. For instance, I used to work at the weekends or in the evenings at or around my PhD.

And the PhD was about...
The PhD was about primality testing and was thus in applied number theory with an explicit application to cryptography too. It was completed during my time at the bank. I then liked designing efficient algorithms. Some of the ideas from that time came to fruition later, for instance recently in the fastest general primality test for large numbers.

...and as a main occupation

But at some time you decided to move from your industry job into research. Why did you make this decision?
Probably the feeling had accumulated that I wanted to do more mathematics. It happened that I was offered a position at the RSA labs, the research group of a major cryptography company in the USA, and, at the same time, at a university. Doors were open in both directions; in fact, I first went to RSA for several months and after that I accepted the university position, at Paderborn University in Germany. I guess my inner voice told me that I wanted to do academic research and teaching too. In Boston, I was already working at Catalan in the evenings – one may speculate whether this had an impact on my decision too ... it is probably just speculation!

Pa: ***Did the university come to you or did you apply for a university position at this time?***
I corresponded with Professor von zur Gathen (Paderborn University, Germany), who had invited me before to give some seminar lectures on the results of my PhD. We kept in touch after that and in fact he offered me a position that was also connected to some cryptographic applications, yes.

Catalan's conjecture[1]

Let's speak shortly about Catalan's conjecture. How did it come that you were concerned with this particular problem and how did you solve it?
This is more than one question...

Maybe you could tell us how you got involved with the problem and on which scientific shoulders your solution was built upon.
Let's try to break this down into several questions. Firstly, why did I get concerned with Catalan? I came across it at a conference in Rome during an interesting talk by Guillaume Hanrot. Returning to Paris where I was spending a summer doing research, I found myself alone and I worked several days to understand more about Hanrot's methods. I did not stop until I had more than a proof of that conjecture! It happened that within a week or two, I could do a step that was then considered to be non-negligible; I proved the so-called "double Wieferich conditions". That was encouraging and may have strengthened my tenacity. Then I was in Paderborn, where I had the peace of mind to think over a longer period about this problem – it was different from the evenings of mathematics after work.

You were asking about the "shoulders" on which I was standing. I would at first answer that I was jumping from shoulders to shoulders. At the beginning it was the shoulders of various people who had investigated Catalan's conjecture in the last 30 years; there's a long list. After Bugeaud and Hanrot, who gave me a taste for the question, I got acquainted with Maurice Mignotte, who was very active in the area. I had to understand the ideas of Inkeri and Schwarz, and Bennet, Glass and Steiner, Tijdeman, and, of course, the consequences of the work of Baker. At the base of all practical results there was an analytic simplification made by Cassels in the 1950s – everybody needed that result as a starting point. I certainly forget half of the important names... However, today I would claim that the shoulders that still hold the present proof are those of Kummer, Leopoldt and Thaine, who gave the fundamental facts from cyclotomy that are used.

Perspectives of number theory

Catalan's conjecture is in the field of number theory. What are the perspectives of number theory today?
Pa: I'm glad this question has been asked of you. (*smiles*)
Mi: Glorious as ever ... I am sorry; on the one hand, I do not retain the authority to expand on this question – there are much more competent people to do that. And I can imagine they would also be very careful with prognostics. But since I stand here as one who has worked applying mathematics and who has also done research, I would like to recall one impressive example. Algebraic geometry in positive characteristic was born with Weil and Grothendieck (pursuing work done by Dedekind and Weber, and Kronecker and Artin) as I see it – being the amateur expert that I am – in the second half of the last century. It took some time to be established among geometers themselves. In the 80s however, with Schoof's algorithm for fast counting of points on elliptic curves defined over (large) finite fields, the topic became in a short time a domain of intensive research in algorithmic number theory with practical applications in cryptography. It is hard to say where such phenomena happen or predict how they will happen again in the future, but they certainly will!

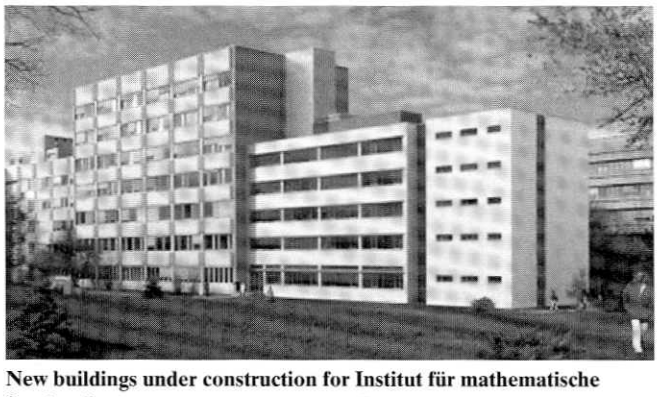
[1] Mihăilescu's theorem (formerly Catalan's conjecture) was conjectured by the mathematician Eugène Charles Catalan in 1844 and proved in 2002 by Preda Mihăilescu. It states that the only solution of the equation $x^a - y^b = 1$ for $x, a, y, b > 1$ is $x = 3, a = 2, y = 2, b = 3$. The proof appeared under the title *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math. 572 (2004), 167–195.

The Göttingen tradition

We are here at the University of Göttingen and, as Professor Munk told me, there's a tradition at this university of combining pure and applied mathematics. Professor Patterson, could you tell us a little bit about the tradition of this university and about the state of art today.

Pa: Well, the origins of mathematics in Göttingen really have to be traced back to Carl Friedrich Gauss, who was the director of the Sternwarte (the observatory here) for a very long period of time. He wasn't actually a professor of mathematics – he was a professor of astronomy – but he was regarded as the leading mathematician in Europe at the same time. So at this point you have someone who was, for example, doing very practical work during the triangulation of the Kingdom of Hannover, and on the other hand developing, using this experience, the abstract area of differential geometry. And the tradition of Gauss has essentially inspired everybody in Göttingen since then, in one way or another. One of the people who took this up most strongly was Felix Klein, who was very, very much involved in the connections between mathematics and industry. He didn't get much gratitude. Such questions were hotly debated about 110 years ago. Klein was involved in a whole series of public arguments. This was part of the development of the Prussian state and industry.

Mathematisches Institut Göttingen at the times of Courant and Hilbert and today



New buildings under construction for Institut für mathematische Stochastik

And at present? Is there some kind of tradition that leads to the present in the university here?

Pa: Well, we are like most universities. We are quite small as a university, as far as mathematics is concerned, but there are three mathematical institutes inside the faculty. One is called, for historical reasons, the Mathematisches Institut, which is merely pure mathematics now, and then there are the two applied mathematics departments: the Institutes for Numerical and Applied Mathematics and the Institute for Mathematical Stochastics. If I may allow myself a personal opinion here, I would like to see, within a reasonable amount of time, all of these under one roof and working together with one another. At the moment this is not about to happen and the present planning is to move to a new building in about nine years.

The perception of mathematics in industry

In your biography you had both: on the one hand, you worked in applied mathematics in industry and on the other hand, you were working in research and now in academia. I would be interested to hear a little bit about how industry views mathematics?

Let me give some partial answers and perspectives. First, there are those domains that are traditional "customers" of mathematics: mechanical and electrical engineering, financial and insurance mathematics and a few more. There, mathematics is probably supposed to be an important tool for the precision and accuracy of the required application and the image of what one can expect from mathematics generally has precise contours. This is simply due to tradition.

And outside these traditional branches?

There have been many more recent applications born with the development of the computer. From statistics and information theory to the very dynamical branches of computer science – they are encountered almost everywhere, from the pharmaceutical industry to transportation scheduling, from the food industry to, say, flood and earthquake prediction.

And what is the reception of mathematics here?

Frankly, I would not know the answer. An educated guess may be that every domain reaches a degree of complexity beyond which the immediate solutions are not sufficient and some mathematical understanding is called for.

And this would then have a positive impact on the image of mathematics!?

In principle, yes, depending on how widespread the awareness is that a change was brought about by mathematics. After all, maybe to a large extent, people in industry care less about the distinctions between various scientific disciplines, as long as things work... Therefore,

there is a difference between the image of mathematics and the image of mathematicians. Maybe the latter is more distinct and I believe they are, in general, well regarded for their ability to structure complex problems, identify possible solutions and modify targets so that they become affordable.

You mean that mathematicians are asked for in industry?
I mean they are well regarded. There is often the principle of learning by doing in industry. You may find a physicist solving integer programming problems or a number theorist becoming a software manager or a bank manager. So, mathematicians have a good reputation for coming around to problems on which they are trained and those for which they are not. They soon have to discover that they belong to a micro-culture to which absence of proof is close to illusion. This is a positive contribution to the collective, especially when they do not expect that the others adhere to the same standards of formal consistency. It is a good habit to explain convictions, even obtained by some proof reasoning, in terms closer to common language. Most people may resent an excess of precision and accuracy of expression as a kind of snobbery.

How did you experience the change from industry to academia?
The time frames are certainly different in industry and it is sometimes hard to pursue an important idea over a longer period of time. My taste and my own history make me long for places where the two meet or it is foreseeable that they could meet. To an extent, I was offered this opportunity in Göttingen for this reason. Here it is possible to pursue both theoretical research in number theory at the Mathematical Institute and practical research in biometrics at the Institute for Mathematical Stochastics.

Biometrics

Mr. Munk, in your institute you work jointly with Mr. Mihăilescu on biometrics. Are there many groups in mathematics that are working on biometrics?
Mu: No – interestingly, this is not the case. Worldwide, there are many groups, either in academia or in industry, who work on that issue, of course, but usually their background is from computer science, in particular pattern recognition or electrical engineering. The group here is, as far as I know, the only larger group in a mathematical department that deals extensively with those issues – and that certainly makes it unique. Indeed, in our group we bring together experts from several areas. Preda Mihăilescu has a background in cryptography, on the one hand, and on the other hand, in biometrical identification analysis. We combine his expertise with my statistical knowledge and our knowledge in pattern recognition, image processing and enhancement and specific aspects of geometry. Actually, our research process itself gradually increased the insight that many interesting mathematical questions are inherent to biometric issues.
Mi: There is a nice historical analogue to what we are doing. At the beginnings of data transmission with modems, the data were transmitted in clear text and the transmission rate was low. There is a fundamental law of information theory, Shannon's law, that states that one cannot transmit data over a channel at a rate beyond the so called "*channel capacity*", which is essentially limited by the physical channel used: wires, radio, etc. That physical limitation was hard to relax, so nobody knew how to reach better transmission rates for modems. Some people believed this was not possible without improving the physical channels – and that belief was scientifically backed up by Shannon's law. Yet, Liv and Zempel looked at the problem from a different perspective and found that one does not have to send more text at a time in order to increase the rate. It suffices to increase the information that the text contains – and for this, one can compress the text before sending it on the physical channel and then decompress it, since in fact most of the data sent over the net have a high rate of redundancy! By using compression, the transmission rate suddenly increased, without changing the physical channels and without contradicting Shannon's law.

Fingerprints

Mi: In fingerprint security we are in a somewhat similar situation now. Our group has proved that the security based on the currently used fingerprint data is bounded and in fact insufficient. Using presently extracted data, one can – by state of the art methods – never reach the degree of security required for internet transactions. The proof is based on statistical evidence from the literature, evidence we want to back up by our own extended field research. But the order of magnitude is quite reliable. So, by changing the perspective, as Ziv and Lempel did, one is led to the observation that the finger contains a wealth of information that is currently not used in AFIS (Automated Fingerprint Identification Systems). The human operator uses this passive information, so she can sort out evidence in cases in which the machine does not. Obviously, we need new algorithms capable of extracting and structuring such information; this will also increase the security rate. This was one major goal for our group from the start. We first thought only of improving the identification rate – now it shows that the same work can help improve the security systems based on biometry.

I think it would be interesting for the readers to describe the different credentials that are present in the Institute for Mathematical Stochastics; moreover, what are people actually working on?
Mu: In fact, we combine the expertise of various people with different backgrounds. As I said before, Preda Mihăilescu has an expertise in cryptography and practical biometrics. Then we have somebody whose background is from differential geometry, obviously an area of pure mathematics, that turns out to play a very important role in the modern analysis of fingerprints. My own background is statistics; we have people with a degree in computer science and even a degree in both computer science and

Screenshot from fingerprint development and analysis software

mathematics. We collaborate with people from physics and from biology. This makes such an area more attractive for me personally; it is interdisciplinary in the true sense.

At the end of the day, I think mathematical modelling plays a very important role, and this can and has to be done by mathematicians. This is probably the particular strength of our group: we tackle various applications from the perspective of mathematics. Our major focus is mathematical modelling and the understanding of mathematical structures that we use for fingerprint identification, for example. This is then combined with statistical issues, e.g. the investigation of the distribution of the main characteristics of a fingerprint on the finger. Just view your own finger tip and you experience a nice flow field of ridges and bifurcations with fascinating random patterns – a living geometry!

Human vs. machine expertise

Talking about biometrics, where do you see the major challenges in the near future where mathematical ideas will make the difference?

Mu: An important issue, which I think will play a major role in the next few years in the whole area, is the intersection between biometric identification systems and security issues, i.e. security issues in the sense of cryptography. Here, Preda will certainly play a prominent role in our group. Furthermore, statistical ideas are required. Traditional cryptography uses reproducible information – any password or secret key is a unique chain of characters from an alphabet. In contrast, fingerprints have an inherent variability that has to be taken into account and cannot be avoided. This leads to a paradoxical situation: security under variability of the key. This seriously limits the potential security of biometrical systems! It appears that the state of the art approaches are unaware of this limitation in various applications, in particular in 'soft biometrics', where time and money often imposes restrictions to security. However, I believe that a combination of thorough statistical understanding of these limitations and innovative use of additional fingerprint information, which so far has been neglected as well, will improve both reliability and security of such systems – a great challenge for the future! It is by thorough understanding of the nature of limitations that one can, like in the case of Liv and Zempel, find a way to bypass them.

Mi: I'd like to add that this is a domain of an intellectual nature where there is some unknown mathematics. It is interesting that computer scientists who have worked in "expert systems" have repeatedly faced the problem of learning from human experts. Some simple general rules can be easily understood and transformed into algorithms but then running "man against machine" on some specific decision problem, one finds that human experts tend to be better, yet they cannot explain to the computer scientist the choices behind their decision processes. This is a complex problem and certainly the human has a wide capacity to integrate – let me use the word *holistically* – complex, even apparently irrelevant data, and therefore improve the decision. We are thus trying to improve the algorithmic integration of the layers of information by learning from humans. If we make some step ahead in this direction, certainly the immense processing capacity of the computer will then make it possible to use the machine for double-checking expert decisions in critical contexts; experts do make errors too!

Mathematics has the capacity of modelling. Situations like this one teach us a certain kind of humility, since the major, powerful tools of mathematics don't get to the facts. There is a need for some interaction with the object that approaches a mathematical and machine understanding of what man was doing before. We are in this process, and it brings up new notions and new ideas, which then offer a feedback to the possibility of bringing more well-known – or possibly new – domains of mathematics into the game. We are at this turning point.

Can you give an example of what man did before the machine?

Yes, certainly. If you look at fingerprints, it was defined in a somehow conventional way that the so called minutiae identify the fingerprint and thus the person. Minutiae are, for instance, line endings and line bifurcations on the finger. Matching sufficiently many of them (12–18, say, according to domestic laws of various countries) identifies a person in court. However, an expert looks at the whole image of the finger and he uses everything he sees there for the orientation and thus for the matching of minutiae. The machine was (essentially) only taught to use the actual location of minutiae. So the integrative process will probably need to take ridge connections, curvatures and further visual impressions into account, which the expert may use in case of uncertainty.

Mu: But there is another aspect, and maybe this clarifies why we require this broad range of expertise: from statistics, imaging, pattern recognition and cryptography. If you, for example, simply raise the question of how secure a fingerprint identification system can potentially be, various issues have to be considered. One is the pattern recognition part, which means how accurate the informa-

tion is that the algorithms extract in order to optimize the identification rate. The other issue, and no machine can answer this question, is how good the quality of fingerprints are in nature in order to make these things work, i.e. what are the inherent natural limitations of the achievable error rates in biometrics. This is not very well understood, albeit of great practical relevance.

For example, we have recently started a project with the Bundeskriminalamt – the German Criminology Agency – where we investigate statistically how fingerprints transform over a lifetime. There appears to be a problem in quality with prints of elderly people and very young people. Fingerprints change during relatively short time periods in these age groups and this is not understood at all.

This causes difficulties for the minutiae – based approach, which is used in AFIS nowadays, because there is some physical distortion of the finger, especially with teenagers. It is not easy to identify the same person over a gap of two to three years because of finger growth. But you can do it if you use the background information that we are extracting, since the line connections are still the same; it is just the rectangular reference grid of the minutiae that is distorted, like one of those popular paintings of Vasarely.

Pa: ***I'm just wondering here – fingerprints have been used for 100 years. Was this not a problem before now?***
Mi: As I explained, the human expert had less of this problem. On the other hand, the human can never process the huge amount of data that a machine can. We wish to teach the machine to use more information in uncertain cases and thus approach the differentiated attitude of the human, while keeping its specific high performance.

Mu: And there is another issue that is very important. At the end of the day, the target of your identification system is to guarantee certain error rates, irrespective of the particular method used or even of the fact that human experts are involved or not. However, the requirements set for these error rates logically depend on the application. Thirty years ago, fingerprints were mainly used in forensics but nowadays we are talking about fingerprint identification in a variety of applications, including commercial systems like access control to personal computers or cell phones, where the security does not need to reach forensic standards. In contrast, other commercial applications involving financial transactions require very low error rates and are only just developing.

Security issues

A particular problem of your research is probably to estimate the security of biometrical systems?
Mu: How secure is the method? Certainly, we are investigating the limitations of technologies. To be more constructive, we believe that we can occasionally bring some new mathematical ideas into the business, which really can help to improve the identification systems – and which to some extent also explore the possible limits of technologies.

Mi: As I said, some leading methods that are currently proposed have insufficient security. I explained why we are optimistic about the possibilities of improvement. It belongs to the purpose of research that one tries to prove lower bounds to the security that one can offer. This requires more work (in statistical modelling too). It is a difficult task that we take upon us.

But we cannot provide the certainty that a deployed system doesn't have gaps in the security conception and guidelines. The conception of the system is very important and it has to reduce the risks in a hierarchical structure. I know from earlier experience in the industry that security is not only a matter of the cryptography used but also of the risk hierarchies. The first project I developed was the security of online ATM systems in Switzerland. There you have a hierarchy of keys and the ultimate keys are, by design, unknown to anybody. They are born, kept and used in a tamperproof security box. This is a computer whose memory is instantly deleted when you shake it or physically tamper with it. The next hierarchy of keys are known to a very few well-trusted people, etc. Actually I believe that the management did not completely trust this technology, so they also printed out the core key, making it accessible to a designated bank director; maybe this is better. However, the most important keys should be known to a minimal number of people. This is a matter of design; it's not a matter of cryptography or of biometrics.

There is a very strong connection between this research and the applied aspect, the aspect of concrete applications in industry, in bank systems. You told us that the mathematical aspect is very important in biometrics. Are there concepts or aspects that you can take from pure mathematics and then apply in your research? Could you describe some of these?
Mu: In our institute, we are of course not only concerned with biometrics. To give you an example, we have recently started to work on growth modelling of biological objects such as trees and leafs. This is supported by the German Science Foundation and we collaborate closely with colleagues from the forest science department, who perform field experiments. This practical problem has initiated fundamental research towards principal component analysis on manifolds, which we call geodesic principal component analysis. Here we benefit a lot from discussions with colleagues from differential geometry and optimization.

Mathematics and Applications

Pa: There's one comment I'd like to make on this: the notions of pure mathematics and applied mathematics are not terribly firm or precise. When I was a student, applied mathematics was very much associated with physics but what is now stated as applied mathematics, for example in cryptography, is very, very much what in those days was considered as pure mathematics; it was number theory. Number theory was considered, let us say, in the late 1960s as one of the purest areas of mathematics; nowadays it is one of the most applied areas of mathematics.

Mi: Exactly, for instance the algebraic geometry over finite fields that I mentioned.

Conversely, do you think that there is also some payback from applications of mathematics, fostering new theoretical research?

Mi: Mathematics progresses both by the impulse from questions raised in physics – and nowadays from a much wider domain of applications – and from questions arising in the mathematical research itself. An important aspect is that the period it takes for some new fundamental mathematical insight to find an application – a reflection in the sensible world, I would say – is long, usually very much longer than, for instance, the time it takes for a discovery in experimental physics to be translated into a revolutionary technology.

Sometimes, this process is iterative. I am far from being an expert but here I think for instance of Riemannian geometry used in relativity theory, whose further development has continuous impacts on mathematics and physics, as I understand it.

Pa: I think it actually seems to occur on a rather slow, almost geological, time scale. What happens is that you find a student coming up, and she or he learns two or more different areas either from different teachers or from books or something like that and then brings them together in her or his person. And then the development takes place. Each generation of mathematicians has got this essentially dialectic aspect that brings together new connections and this is exactly what keeps mathematics alive. Just as a single line, it would die out.

Public awareness – in Germany

2008 is the year of mathematics in Germany. How do you think the awareness of mathematics is in the real world, in the public?

Mu: Personally, I would say that a major challenge for the mathematical community is to focus the attention of society on the benefits it draws from mathematical research. When something in mathematics is invented, typically it takes a very long time until it is recognized in society as a value or a contribution. Moreover, when a mathematical result is at the heart of a practical invention it is not recognized as such anymore. In other disciplines this goes faster and this process is much more direct. Inventions in molecular biology or in medicine, let's say, are first of all recognized as inventions of these disciplines. At the beginning of the 20th century Radon developed what nowadays is called the Radon transform, and about 60 or 70 years later people used it for tomography. Of course, nobody in the public related these two things anymore. And there are many other examples: the mathematics of financial markets that is used in every investment bank nowadays is founded on the famous Ito-calculus from the early 50s, which itself is based on Brownian motion developed by Einstein and Wiener in the first quarter of the last century. This has been very successfully applied in the 70s to option pricing, and the Noble prize in economy was awarded for this development. These very long periods of time prevent the public from appreciating the value of mathematics and how it really matters to us.

Pa: Can I say something about my experience here? Much of modern mathematics started in Germany during the 19th century and it came to me as a huge surprise to discover how negative many people in Germany are about mathematics. It is a very strange experience: when one says one is a mathematician here, one usually gets the answer, 'I was never any good at mathematics at school,' or something of this nature. In fact, the attitude is quite different, let's say, in the UK or in France where there are many programs in the media about mathematics, on the BBC or in other places. We've just been involved here in a program that is being made by Marcus du Sautoy for the BBC. One might hope, though it's a rather weak hope, that in the course of the Year of Mathematics one might actually change this a little; it seems to be a specifically German attitude that you do not find in other countries.

May I come to my last question – do you think that the special work you're doing in biometrics, which combines some aspects of academics and some aspects of industry and applicability may have an effect on the recognition of mathematics in the public?

Mi: If it succeeds in reaching the goals that we have set... Our goals are to improve technological systems, on the one hand, and to develop some theoretical models that can prove something positively in areas that are poorly understood, on the other hand. Maybe the best hope is that solutions found for this specific problem may call for some new mathematics, if we develop concepts that can be used in similar problems. This is the best I can hope for, and then let the waves go the way the waves go. It's always a matter of who hears at the other end of the channel. It's never the whole public.

Hanno Ehrler [hanno.ehrler@gmx.de] studied musicology, art history and ethnology in Mainz. He works in part as a freelance journalist for the Frankfurter Allgemeine Zeitung (FAZ) and the public German TV station ARD (subjects: contemporary music, science fiction, modern technologies).

Axel Munk [munk@math.uni-goettingen.de] is a professor at the Institut für Mathematische Stochastik at Göttingen University. His research in statistics focuses on nonparametric regression, medical statistics, statistical inverse problems and imaging, statistical modelling and shape analysis. Within pattern recognition, he is mainly interested in the analysis of fingerprints.

Samuel J. Patterson [sjp@math.uni-goettingen.de] is a professor at the Mathematisches Institut, Göttingen University. His main research areas comprise analysis on and around Kleinian groups, generalized theta functions and metaplectic groups, and analytic number theory in general.