UNIVERSITÀ DEGLI STUDI ROMA TRE

Dipartimento di
Matematica

Largo San Leonardo Murialdo 1
00146 Roma (Italia)

Report on the CIMPA – UNESCO – Nepal School
"*Number Theory in Cryptography and its applications*"
School of Sciences, Kathmandu University, Dhulikhel, Nepal
July 19 – 31, 2010

This report arrives as last after those submitted by Kanhaiya Jha and Michel Waldschmidt available in the web at:

1. http://ku.edu.np/pdf/ReportonCIMPASchool2010.pdf
2. http://www.math.jussieu.fr/~miw/articles/pdf/RapportMissionCimpaNepal2010.pdf

I refer to these documents in order to avoid repetitions. The idea of a CIMPA school in Nepal had its origin during my visit to Kathmandu University in December 2005. In that occasion, I met Kanhaiya Jha for the first time. I was introduced to him by Kalyan Chakraborty from HRI (India).

The final balance of the project is, in my opinion, positive. This success is due primarily to the massive amount of passion and work of the local organizer Kanhaiya Jha. Furthermore the constant and active collaboration of Michel Walschmidt has also been crucial in the organization. Michel's work had as consequences: the recognition of the school as a satellite event of the ICM, funding from NBHM to support the travel expenses of the Indian participant, funding from the Abdus Salam School of Mathematical Sciences in Lahore to support the local expenses of the Pakistani participant and several more. Finally without the professional and always prompt assistance of Agnès Gomez and Jeanick Allanic the project could not have succeeded. I would also like to thank the CIMPA director Claude Cibilis for his availability and involvement it the organization.

I found the roadmap extremely useful and I feel that its expansion and improvement could be even more useful for future CIMPA schools.

My remarks will mainly focus on the scientific aspects of the school since the other report give a complete account of other aspects that I entirely subscribe. In the original plan, the number of speakers was higher but due to various reasons, several invited lecturers had to cancel their participation. Nevertheless the final number of lectures was quite large and the program significantly rich.

SUCCESSFUL POINTS

Most of the lectures were well coordinated. Some basic concepts on primality testing and factoring were repeated in several lectures and in different contexts and this provided occasion the elaborate concepts from various angles. It is appropriate to say that r*epetita iuvant.*

The atmosphere was extremely constructive and I think that the various students merged well together. I think that some of the contacts that have been established will grow into future scientific and personal collaborations.

☎ [+39] 06 5733 8243 **FAX:** [+39] 06 5733 8080 ✉ pappa@mat.uniroma3.it

I am convinced that the Mathematica labs held by Corrado Falcolini were extremely useful and on this point I need to spend a few words.

It is widely believed that the computer assisted teaching is more effective then the traditional one. I partially agree with this point of view but in the case of Mathematics and particularly in the case of algorithmic number theory, being able to implement ideas and theoretical algorithms while studying them, can have terrific consequences. Using large numbers and seeing them used for elaborate computations sometimes allows to absorb the theory behind the algorithms much quicker.

In a short and intense school like the CIMPA one, I felt that it was very important that students had this opportunity. The choice of using the Wolfram Mathematica package looked appropriate partly because of its friendliness for users and partly because I was hoping in a more significant involvement of Wolfram in the project. In fact Wolfram offered to provide free licences during school and for a period after the conclusion of the school.

Unfortunately, the installation of the licences turned out to be much more complicated than expected and it took two entire days of work by at least four persons. But at the end, we had a functioning laboratory. We could not use the licences originally promised by Wolfram and we had to install the Roma Tre licences in the lab. Hopefully these licences will be active until next June 2011 but this is not guaranteed.

It may be argued that it has no sense instructing students from a developing country to the use of an expensive and non free software. However the same is true for science in general. Access to advanced libraries is in general difficult in these nations but this should not be a reason not to provide advanced teaching.

If I should organize again a similar school, I would propose a similar laboratory. I feel that some pressure should be put on companies like Wolfram to support more significantly events like CIMPA schools providing free licences to universities in developing countries for long periods (e.g. 5 years). Another option is to adopt free packages like SAGE that would not need any licence. But in conclusion, I think that lab sessions are important.

Another successful aspect of the school is the attendance of young participants from developed countries. Their presence was positive in several ways. They were either graduate students or young faculties in European or American universities. Some had some experience with the use of Mathematica and could be of great help during the labs. Some knew already the material covered in some of the courses and could act as connectors between the lecturers and the other participants. Some simply enjoyed studying new mathematics in a pleasant environment like Kathmandu University. I feel that in future schools, as long as they are able to find independent financial support, the presence of young graduate students from Europe is desirable.

The structures offered by Kathmandu University were highly satisfactory. Once again I should mention how effective the work of Kanhaiya has been in this respect. The Campus is in breath taking location and the only problems took place in the KUIC (Kathmandu University International Centre) where the lack of electricity in the evening made it difficult for the international participants to study and interact at night.

☎ [+39] 06 5733 8243 **FAX:** [+39] 06 5733 8080 ✉ pappa@mat.uniroma3.it

WEAK POINTS

It is honest to say that most of the weak points in the NEPAL school are due to my lack of experience with organizing an event of this type. If I had to organize a similar event now, I would certainly be more effective and would change several of my choices. First of all I would propose a larger scientific committee that includes more mathematicians with experience in programs of this sort. Without the cooperation of Michel Waldschimt that was not in the scientific committee, the project would have been much more complicated or impossible to organize. I would also like to mention the decisive conversations with Kalyan Chakraborty. They were really important and I regret not to have added his name in the scientific committee especially since he was one of the conceiver of the project.

Uncertainty about the budget took away some of the effectiveness of the organization. We were always reluctant in committing ourselves with expenses that inflate the budget. More courage in certain stages would have been better. In part this caused some misunderstanding with some of the invited speakers that cancelled their participation probably also because of my limited or evasive communication.

There were too many lectures and too little time left to the students to interact. In this respect the observations from the participants quoted at the end of the report from Michel Waldschmidt are justified. If I had another chance to organize a CIMPA school, I would restrict the lectures only to the mornings and intensify the tutorials and labs in the afternoons.

Some of the lectures were advanced and, I am afraid, they were too difficult for most of the students. As already mentioned in other reports, the level of the students was too diversified with the obvious consequences in terms of understandings. Recruitment of the lecturers and their instruction on how to deliver their lectures should have been more effective.

FOLLOW-UPS

It is of major importance that intelligent follow-ups of the CIMPA school are organized soon. One of the Nepalese students after the end of the school asked me: “now that the school is over, that we became interested in Number Theory and Cryptography, what should we do next?”

Nepal is a fertile country also in terms of the growth of a mathematical community that could contribute to its future. Several colleagues both from Kathmandu University and Tribhuvan University requested active cooperation for the future years including the possibility of teaching courses in their departments. A memorandum of understanding has been signed from the Vice Chancellor of Kathmandu University and the Rettore of the Università Roma Tre. Under this umbrella more activities will be promoted. I am in the process of applying for cooperation funding from the Italian Minister of Foreign Affairs to sponsor some future collaboration. At the same time it would be desirable that some Nepalese students are given the opportunity to visit European universities and that those with talent, study abroad for PhD. Note that there is not any established PhD program in Mathematics offered by Nepalese Universities.

☎ [+39] 06 5733 8243 **FAX:** [+39] 06 5733 8080 ✉ pappa@mat.uniroma3.it

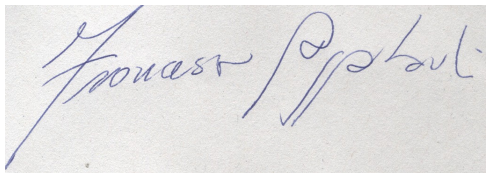
Some of the follow-ups already started immediately after the end of the CIMPA school. Roberto Ferretti, one of the three Italian speakers was invited to deliver a colloquium at Tribhuvan University by Min Khati from the Computer Science Department. Corrado Falcolini gave a series of Mathematica laboratories at Global College of Management and finally Elena Prestini from Università di Roma Tor Vergata is now visiting Tribhuvan University. My next visit to Nepal of December 2011, is already mentioned in Michel's report. I will try to visit Nepal earlier.

As for the role of CIMPA in the follow-ups, I feel that in a few years another CIMPA school should be organized in Nepal. Before that one or more programs like the NSNTC could take place.

The National School on Number Theory and Cryptography (NSNTC – 2009) took place at Kathmandu University from December 26, 2009 to January 05, 2010. For some Nepalese students, that event was more effective as its level and contents were sized expressly for the audience.

If Kanhaiya Jha or some of his Nepalese colleagues are willing to organize another National School in the future, it would be excellent if CIMPA could provide some sort of support. I am certainly willing to participate.

Yours sincerely



Francesco Pappalardi

☎ [+39] 06 5733 8243 **FAX:** [+39] 06 5733 8080 ✉ pappa@mat.uniroma3.it