CIMPA School Final Report

Elliptic Curves and their Applications

July 14, 2025 – July 26, 2025

Institute of Mathematics, National Academy of Sciences of Armenia,
Yerevan, Armenia

The organizers are grateful to CIMPA for its generous support, and to the Institute of Mathematics of the National Academy of Sciences of Armenia for hosting the event. We also thank all lecturers and participants for their contributions to the success of the school.

1. Summary

The CIMPA Summer School aimed to introduce students and early-career researchers to the fundamentals of elliptic curves and their applications in contemporary number theory and cryptography. The program was highly successful, bringing together participants from twelve countries. Students engaged actively in lectures and problem sessions, collaborated in small-group research projects, and concluded the program by delivering presentations on their results, demonstrating both enthusiasm and meaningful progress. The research projects initiated during the summer school have the potential to lead to formal publications. Looking ahead, and contingent upon the availability of funding, we anticipate the possibility of organizing a follow-up meeting to bring participants together again and further advance these collaborations.

2. Scientific Content

The summer school included four mini-courses:

1. **Introduction to Cryptography**
   Instructor: *Diana Davidova* (Institute of Mathematics of the National Academy of Sciences of Armenia)
   Description: This course introduced symmetric and asymmetric cryptography concepts, their differences, advantages and disadvantages, and provided a brief historical overview of cryptography (from ancient times to WWII and modern cryptosystems). Symmetric cryptography was discussed in more detail, in particular block ciphers. The algebraic properties of block ciphers that guarantee their security against different types of attacks were studied.

2. **Introduction to Elliptic Curves**
   Instructor: *Mihran Papikian* (Pennsylvania State Unievrsity, USA)
   Description: This course introduced the concept of elliptic curves, the group structure on points of an elliptic curve, endomorphisms, torsion points, the Weil pairing, and elliptic curves over finite fields, culminating with a proof of Hasse's Theorem.

3. **Elliptic Curves and Modular Forms**
   Instructor: *Valentijn Karemaker* (Utrecht University, Netherlands)
   Description: The course provided an introduction to the deep connections between elliptic curves and modular forms, as exemplified by the proof of Fermat's Last Theorem and subsequent research in this area. It began with the theory of modular forms, covering modular groups and lattice functions, assuming only basic complex analysis. The course then explored the connections between modular forms and elliptic curves through Hecke operators, L-functions, and modular curves, with a focus on explicit examples where these relationships became most apparent.

4. **Elliptic Curves and Cryptography**
   Instructor: *Fabien Pazuki* (University of Copenhagen, Denmark)
   Description: The course focused on elliptic curves over finite fields, which are central objects in modern cryptography. Two main aspects were highlighted: the group structure of rational points and isogeny graphs. In both cases, a solid understanding of the endomorphisms of elliptic curves proved to be crucial. The course emphasized these endomorphisms and showed that, even though the cryptographic applications concern curves over finite fields, a substantial understanding of algebraic number theory and quaternion algebras was required.

The daily program of the summer school typically consisted of three 60-minute lectures and three 50-minute exercise sessions. The lectures emphasized carefully worked examples rather than formal proofs, providing participants with concrete illustrations of the material. During the exercise sessions, participants worked in small groups on a set of assigned problems, receiving guidance and hints from the instructor when needed. Solutions were discussed collectively at the end of each session. Several exercise sessions focused on computational mathematics, where participants were introduced to software such as SageMath and Magma and engaged in exploratory, open-ended experimentation.

In addition to lectures and exercise sessions, participants were divided into groups of five to eight students and worked on projects under the supervision of one of the instructors. Dedicated time slots were provided during the second week of the school for these groups to meet and discuss their projects. On the final day, each group delivered a 30-minute presentation on their work. The projects were the following:

- Graph classification of bent Boolean functions in dimension 4 (Diana Davidova)
- Modular forms and elliptic curves (Valentijn Karemaker)
- Maximum Rank Distance Codes, Semifields, and Drinfeld Modules (Mihran Papikian)
- Distortion maps for the Weil pairing (Fabien Pazuki)

Finally, a number of seminar talks were given by participants to present ongoing research projects or recent results.

3. Participants

The school brought together 29 students and early career researchers from 11 countries, including 8 from the host country. Five of the students were women; however, none were from the host country. We note that the initial number of accepted female students was higher–8 out of 28–including two from Armenia, although they were ultimately unable to attend for various reasons.

Foreign participants supported by CIMPA: (with CIMPA application numbers and gender)

13139 (M) Hasan Yilmaz — 1st year M.Sc. student in Mathematics, Bogaziçi University (Turkey). *Email:* hasan.yilmaz1@std.bogazici.edu.tr

14478 (M) Sevag Büyüksimkeşyan — 5th year B.Sc. student in Mathematics, Istanbul Bilgi University (Turkey). *Email:* simkesyansevag@gmail.com

14743 (M) Nikita Andrusov — 3rd year B.Sc. student, Moscow Institute of Physics and Technology (Russia). *Email:* andrusov.n@gmail.com

14977 (M) Erenay Boyalı — 5th year B.Sc. student in Mathematics, Istanbul Bilgi University (Turkey). *Email:* erenay.boyali@hotmail.com

15090 (M) Amin Abedini — 3rd year B.Sc. student in Mathematics, Sharif University of Technology (Iran). *Email:* aminabedini.math@gmail.com

15269 (F) Mona Batrouni — 1st year M.Sc. student, American University of Beirut (Lebanon). *Email:* mab108@mail.aub.edu

15369 (F) Begüm Gülgen — 4th year undergraduate student, Izmir Institute of Technology (Turkey). *Email:* begumgulgen35@gmail.com

15474 (M) Barbod Bahiraei — 4th year B.Sc. student in Mathematics, University of Tehran (Iran). *Email:* barbodbahiraei@yahoo.com

15518 (F) Paria Jamshidi — 1st year Ph.D. student, University of Tehran (Iran). *Email:* pariajamshidi2008@gmail.com

15593 (F) Mahabba El Sahili — 1st year M.Sc. student in Mathematics, American University of Beirut (Lebanon). *Email:* mae160@mail.aub.edu

15606 (M) Gleb Savelev — 3rd year B.Sc. student (Applied Mathematics and Computer Science), Admiral Makarov State University of Maritime and Inland Shipping, Saint Petersburg (Russia). *Email:* gleb.savelev26@gmail.com

13504 (M) Mustafa Kazancıoğlu — 1st year Ph.D. student in Mathematics, University of Groningen and Sabancı University (Turkey). *Email:* mustafa.kazancioglu@sabanciuniv.edu

14152 (M) Jiping Zhang — 1st year M.Sc. student in Mathematics, Higher School of Economics (Russia). *Email:* tszichzhan@edu.hse.ru

12725 (M) Rahim Rahmati-Asghar — Ph.D. in Mathematics (2012), University of Tehran (Iran). Current affiliation unknown. *Email:* rahmatiasghar.r@gmail.com

15515 (M) Bikram Misra — 3rd year Ph.D. student in Mathematics, Indian Institute of Technology Delhi (India). *Email:* Bikram.Misra@maths.iitd.ac.in

15279 (M) Mohammad Zaman Fashami — Ph.D. (2019), currently seeking to transition to number theory. *Email:* zamanfashami65@gmail.com

Foreign participants without CIMPA support:

13338 (M) Dimitrios Noulas — 2nd year Ph.D. student in Mathematics, University of Athens (Greece). *Email:* dnoulas@math.uoa.gr

14603 (F) Flora Benedek — 1st year Ph.D. student in Mathematics, Pennsylvania State University (USA). *Email:* fmb5296@psu.edu

– (M) Bo Rao — Master's student in Mathematics, University of Paris 13 (France). *Email:* rbmath2023@outlook.com

– (M) Hany Hilal Gerges — Ph.D. student in Mathematics, Vilnius University (Lithuania). *Email:* hany.gerges@mif.stud.vu.lt

14791 (M) Jordi Vilà Casadevall — 1st year Ph.D. student in Mathematics, University of Bristol (UK). *Email:* jordi.vilacasadevall@bristol.ac.uk

Local participants:

13345 (M) Arman Bayramyan — 2nd year Ph.D. student in Mathematics, Yerevan State University. *Email:* abayramyan2000@gmail.com

14500 (M) Hayk Karapetyan — 3rd year undergraduate student in Mathematics, Yerevan State University. *Email:* 4966508hayk@gmail.com

14572 (M) Gagik Melkumyan — 2nd year M.Sc. student in Mathematics, Yerevan State University. *Email:* gagik23042001@gmail.com

14629 (M) Ruben Hambardzumyan — 3rd year undergraduate student in Mathematics, Yerevan State University. *Email:* rubenhambarcumyan@gmail.com

14835 (M) Tigran Hakobyan — Researcher in Mathematics, Yerevan State University (Ph.D. 2018). *Email:* haktigran.1@gmail.com

15212 (M) Karen Mkrtchyan — Student in Computer Science, Yerevan State University. *Email:* karenmkrtchyan2001@mail.ru

15528 (M) Gor Melkumyan — 4th year undergraduate student in Mathematics, Yerevan State University. *Email:* gormelqumyan6@gmail.com *Note:* Participation unconfirmed.

15576 (M) Gevorg Hunanyan — 1st year M.Sc. student in Mathematics, Yerevan State University. *Email:* gevorg.hunanyan.999@gmail.com

All accepted students demonstrated strong academic ability and enthusiasm for pursuing mathematical research. **The following students were highlighted by the instructors as particularly impressive during discussions:**

14629 (M) Ruben Hambardzumyan — 3rd year undergraduate student in Mathematics, Yerevan State University. *Email:* rubenhambarcumyan@gmail.com

14791 (M) Jordi Vilà Casadevall — 1st year Ph.D. student in Mathematics, University of Bristol (UK). *Email:* jordi.vilacasadevall@bristol.ac.uk

14152 (M) Jiping Zhang — 1st year M.Sc. student in Mathematics, Higher School of Economics (Russia). *Email:* tszichzhan@edu.hse.ru

15269 (F) Mona Batrouni — 1st year M.Sc. student, American University of Beirut (Lebanon). *Email:* mab108@mail.aub.edu

14743 (M) Nikita Andrusov — 3rd year B.Sc. student, Moscow Institute of Physics and Technology (Russia). *Email:* andrusov.n@gmail.com

4. Financial Report

Funding Agency	**Amount (EUR)**
CIMPA (15000 EUR)	15,000
Scientific Committee of the Republic of Armenia ($3500 $\approx$ 3255 EUR)	3,255
International Mathematical Union (2500 EUR)	2,500
Number Theory Foundation ($2000 $\approx$ 1860 EUR)	1,860
Journal de Théorie des Nombres de Bordeaux (1000 EUR)	1,000
Journal of Number Theory ($1000 $\approx$ 930 EUR)	930
Total	**24,545**

Table 1: Funding agencies and amounts received (with dollar amounts converted to EUR at approx. 1 USD = 0.93 EUR), ordered by decreasing contribution.

Expense Category	**Amount (EUR)**
Travel support for international participants (developing countries)	7,200
Accommodation + meals at Yerevan State University Guest House (all participants)	7,000
Coffee breaks and lunch (12 days, all participants)	7,200
Social dinner (all participants)	1,500
Excursion	1,200
Conference materials (bags and badges)	400
Total Expenses	**24,500**

Table 2: Main expenses of the summer school.

5. Pictures

Figure 1: Summer school official photo in front of the Academy of Sciences of Armenia

Figure 2: Diana Davidova with the students of her project group

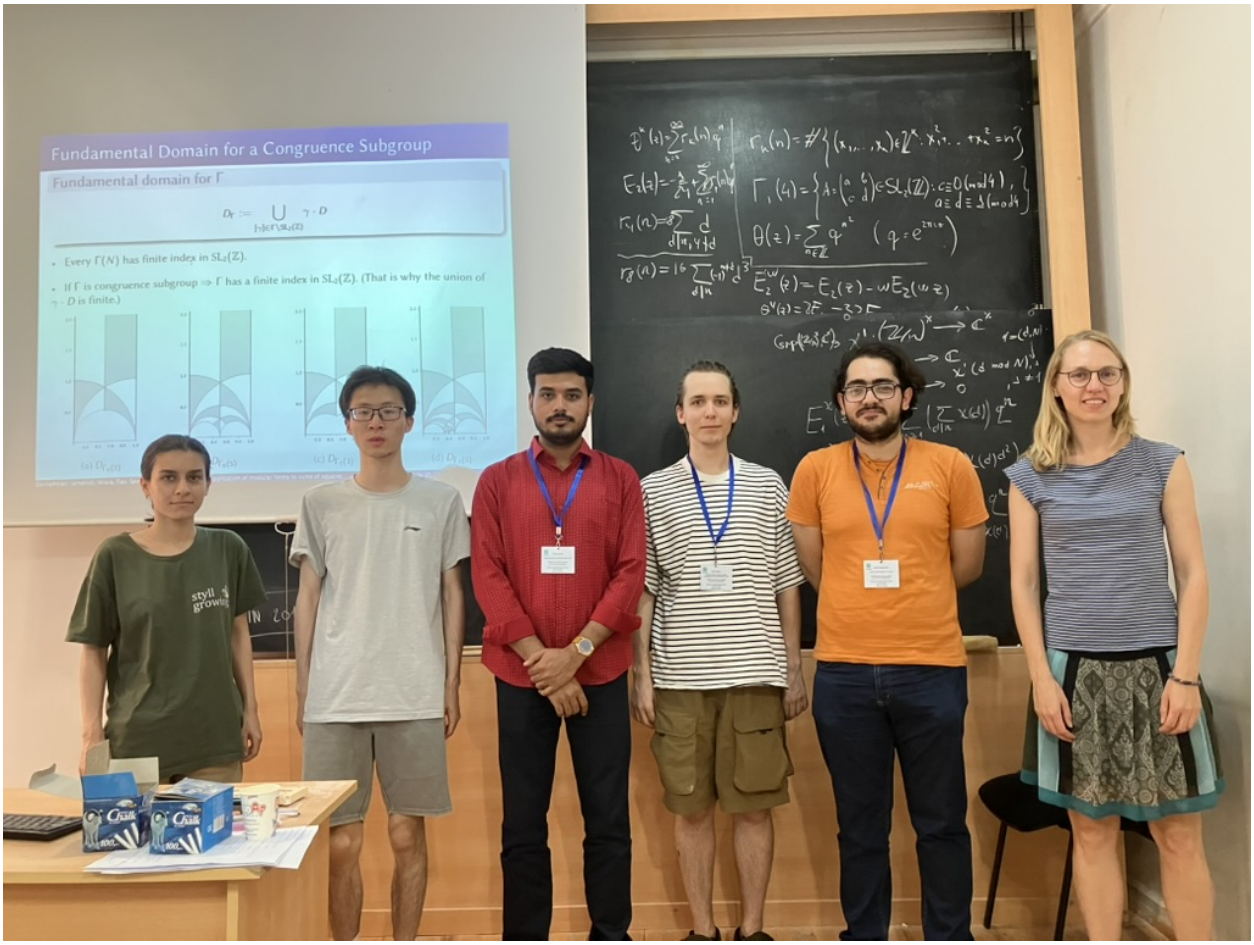

Figure 3: Valentijn Karemaker with the students of her project group

Figure 4: Fabien Pazuki with the students of his project group

Figure 5: Mihran Papikian with the students of his project group

Figure 6: Photo from the excursion

6. Appendix

Appendix contains

- The schedule of the summer school.
- The descriptions of four research projects.

ELLIPTIC CURVES AND THEIR APPLICATIONS

July 14-26, 2025

Yerevan, Armenia

Week 1

Time	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
8:30 - 9:00	Registration and Opening Ceremony					Excursion and Official Dinner
9:00 - 10:00	Introduction to Cryptography	Introduction to Cryptography	Introduction to Cryptography	Introduction to Cryptography	Introduction to Cryptography	
10:00 - 10:30	Coffee Break	Coffee Break	Coffee Break	Coffee Break	Coffee Break	
10:30 - 11:30	Introduction to Elliptic Curves	Introduction to Elliptic Curves	Introduction to Elliptic Curves	Introduction to Elliptic Curves	Introduction to Elliptic Curves	
11:30 - 11:45	Short Break	Short Break	Short Break	Short Break	Short Break	
11:45 - 12:45	Elliptic Curves and Modular Forms	Elliptic Curves and Modular Forms	Elliptic Curves and Modular Forms	Elliptic Curves and Modular Forms	Elliptic Curves and Modular Forms	
12:45 - 14:45	Lunch	Lunch	Lunch	Lunch	Lunch	
14:45 - 15:35	Exercise Session for *EC and MF*	Exercise Session for *EC and MF*	Free Afternoon	Exercise Session for *EC and MF*	Exercise Session for *EC and MF*	
15:35 - 15:50	Short Break	Short Break		Short Break	Short Break	
15:50 - 16:40	Exercise Session for *Intro to Cryp*	Exercise Session for *Intro to Cryp*		Exercise Session for *Intro to Cryp*	Exercise Session for *Intro to Cryp*	
16:40 - 17:10	Coffee Break	Coffee Break		Coffee Break	Coffee Break	
17:10 - 18:00	Exercise Session for *Intro to EC*	Exercise Session for *Intro to EC*		Exercise Session for *Intro to EC*	Exercise Session for *Intro to EC*	

Lectures and Speakers (Week 1)

- *Introduction to Cryptography* (introductory course), Diana Davidova.
- *Introduction to Elliptic Curves* (introductory course), Mihran Papikian.
- *Elliptic Curves and Modular Forms* (intermediate course), Valentijn Karemaker.

Week 2

Time	Monday	Tuesday	Wednesday	Thursday	Friday
9:00 - 9:50	Introduction to Elliptic Curves				
9:50 - 10:00	Short Break				
10:00 - 11:00	Elliptic Curves and Cryptography	Elliptic Curves and Cryptography	Elliptic Curves and Cryptography	Elliptic Curves and Cryptography	Elliptic Curves and Cryptography
11:00 - 11:30	Coffee Break	Coffee Break	Coffee Break	Coffee Break	Coffee Break
11:30 - 12:30	Project Session (with instructor)	Project Session (with instructor)	Project Session (with instructor)	Project Session (with instructor)	Project Session (with instructor)
12:30 - 14:30	Lunch	Lunch	Lunch	Lunch	Lunch
14:30 - 15:30	Exercise Session for *EC and Cryp*	Exercise Session for *EC and Cryp*	Exercise Session for *EC and Cryp*	Exercise Session for *EC and Cryp*	Project Presentation 1 and 2
15:30 - 15:45	Short Break	Short Break	Short Break	Short Break	Short Break
15:45 - 16:45	Exercise Session for *Intro to EC*	Seminar (Vilà-Casadevall and Noulas)	Special Session	Seminar (Hambardzumyan and Fashami)	Project Presentation 3 and 4
16:45 - 17:10	Coffee Break	Coffee Break	Coffee Break	Coffee Break	Coffee Break
17:10 - 18:00	Project Session (only students)	Project Session (only students)	Project Session (only students)	Project Session (only students)	Open Discussion and Closing Ceremony

Lectures and Speakers (Week 2)

- *Elliptic Curves and Cryptography* (advanced course), Fabien Pazuki.

Project Session	Four parallel sessions where groups of six to seven students will work with an instructor on a research project.
Project Presentations 1–4	Four groups of students present the findings for their project, 30 minutes each.
Special Session	Applying to Ph.D. programs in US, Canada and Europe, and the first steps in mathematical research.

Elliptic curves and cryptography

CIMPA research school on *Elliptic curves and their applications*,
University of Yerevan, Armenia, July 14th - July 26th, 2025

– Research project session –

TIME: July 21-25, 2025.

TITLE: *Graph classification of bent Boolean functions in dimension* 4.

STUDENT TEAM:
Mona Batrouni,
Gevorg Hunanyan,
Hany Hilal Gerges,
Begüm Gülgen,
Gagik Melkumyan,
Mohammad Zaman.

SUPERVISOR: **Diana Davidova** (Univ. of Yerevan, davidovadiana210@gmail.com).

ABSTRACT: We will define and study Bent boolean functions. The goal of the project: give a graph classification of bent Boolean functions in 4 variables. How many non isomorphic graphs we will get? How many bent Boolean functions are represented by each of the graph?

Things to take into account

- There are 896 bent Boolean functions in 4 variables.
- All bent Boolean functions in 4 variables are quadratic.
- All quadratic bent Boolean functions are affine equivalent to each other, thus to get all quadratic Boolean functions it is enough to consider one and get others by applying affine permutation. For instance, $x_1x_2 + x_3x_4$ is bent Boolean function in 4 variables (can be easily verified).
- As mentioned above we can divide the set of quadratic bent Boolean functions into classes considering only quadratic part. The functions in each class will have the same graph representation, But functions from different equivalence classes can also have the same graph representation. For $n = 4$ there are 28 classes with 32 functions in each. What are these classes?

Elliptic curves and cryptography

CIMPA research school on *Elliptic curves and their applications*,
University of Yerevan, Armenia, July 14th - July 26th, 2025

– Research project session –

TIME: July 21-25, 2025.

TITLE: *Modular forms and elliptic curves.*

STUDENT TEAM:
Arman Bayramyan,
Paria Jamshidi,
Bikram Misra,
Bo Rao,
Gleb Savelev.

SUPERVISOR: **Valentijn Karemaker** (Univ. of Utrecht, v.z.karemaker@uu.nl).

ABSTRACT: We will study Jacobi theta series and some of their arithmetic applications.

Elliptic curves and cryptography

CIMPA research school on *Elliptic curves and their applications*,
University of Yerevan, Armenia, July 14th - July 26th, 2025

– Research project session –

TIME: July 21-25, 2025.

TITLE: *Maximum Rank Distance Codes, Semifields, and Drinfeld Modules.*

STUDENT TEAM:
Amin Abedini,
Barbod Bahiraei,
Flora Benedek,
Tigran Hakobyan,
Ruben Hambardzumyan,
Hayk Karapetyan,
Hasan Yilmaz,
Jiping Zhang.

SUPERVISOR: **Mihran Papikian** (Penn State Univ., papikian@psu.edu).

ABSTRACT: This project consists of three distinct yet interconnected components: error-correcting codes, semifields, and Drinfeld modules. The project will be dealing with constructing codes explicitly, applying them in cryptographic settings, exploring theoretical frameworks, or bridging theory and practice.

The theory of Drinfeld modules bears a striking resemblance to the theory of elliptic curves, yet it is more elementary and accessible, as it does not rely on algebraic geometry. This project offers a unique opportunity to engage with deep concepts without requiring extensive background knowledge.

More precisely, we will focus on the Maximum Rank Distance codes (abbreviated MRD) and their links to Drinfeld Modules.

Elliptic curves and cryptography

CIMPA research school on *Elliptic curves and their applications*,
University of Yerevan, Armenia, July 14th - July 26th, 2025

– Research project session –

TIME: July 21-25, 2025.

TITLE: *Distortion maps for the Weil pairing.*

STUDENT TEAM:
Nikita Andrusov,
Erenay Boyali,
Sevag Büyüksimkesyan,
Mahabba El Sahili,
Mustafa Kazancioglu,
Dimitrios Noulas,
Rahim Rahmati-Asghar,
Jordi Vila Casadevall.

SUPERVISOR: **Fabien Pazuki** (Univ. of Copenhagen, fpazuki@math.ku.dk).

ABSTRACT: Working with elliptic curves in cryptography has several advantages. For instance, when putting in place a Diffie-Hellman key exchange protocol, here is a reason why using the group of rational points of an elliptic curve over a finite field $\mathbb{F}_q$ instead of the group $(\mathbb{Z}/N\mathbb{Z})^*$ is better. Let $m \geq 2$ be an integer coprime with q. There exists a map with several interesting properties, called the *Weil pairing*, $e_m \colon E[m] \times E[m] \to \mu_m$, where μ_m is the group of m-th roots of unity in $\overline{\mathbb{F}}_q$. This allows to build efficient digital signature protocols.

However, there is a small technical step that needs to be taken care of when putting the setting in place. We will also need a map $\tau \colon E[m] \to E[m]$ such that $\hat{e}_m(P, Q) = e_m(P, \tau(Q))$ defines a non-degenerate map, *i.e.* the kernel should be trivial: $\hat{e}_m(P, P) \neq 1$ if $P \neq 0$. This τ is called a *distortion map*. It is also a fact that $\hat{e}_m$ is bilinear.

As a research activity, we formulate the following question: when can one ensure the existence of such a distortion map? List some interesting examples. (One may use early work of Denis Charles as inspiration.)