SEAMS School Manila 2017 : Topics on Elliptic Curves

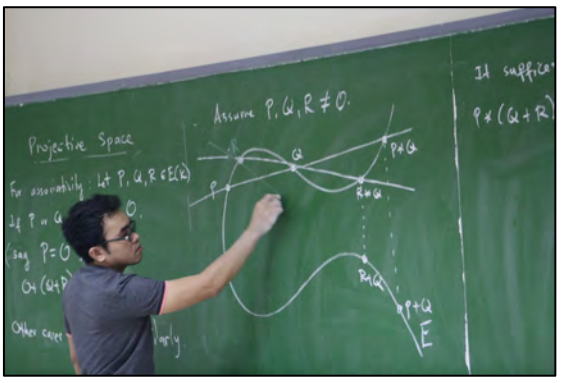
17 – 25 July 2017

Institute of Mathematics

University of the Philippines Diliman

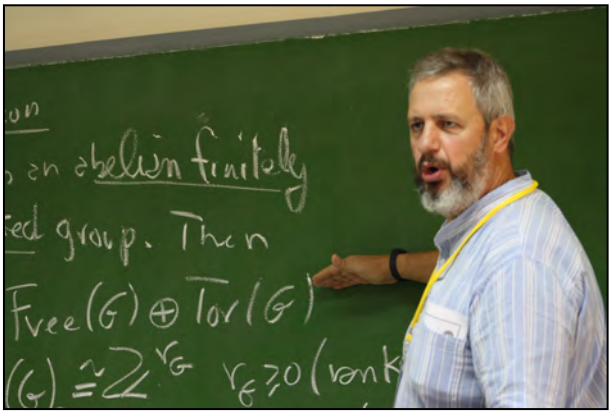
TERMINAL REPORT

The 2017 SEAMS School Manila on Topics on Elliptic Curves was held on 17 July to 25 July 2017 at the Institute of Mathematics, University of the Philippines Diliman, bringing together 48 mathematicians, graduate students and number theory enthusiasts from 9 countries (including 8 lecturers) for a 7-day intensive workshop. The school consisted of lectures, discussions and a computation session on various theoretical, applied and computational aspects of the theory of elliptic curves. The members of the SEAMS School Manila 2017 Scientific Committee were Jerome Dimabayao, Fidel Nemenzo and Michel Waldschmidt.



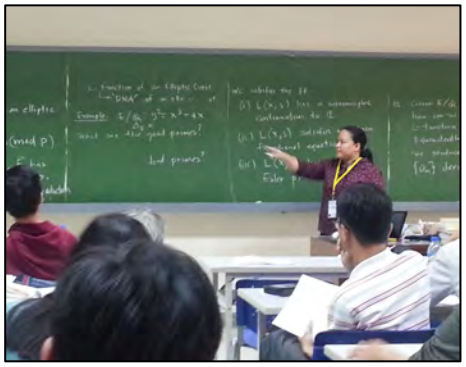
The school opened with introductory lectures on the basic theory of elliptic curves; covering basic algebraic, geometric and analytic concepts such as: elliptic curves over arbitrary fields, the group law on rational points on elliptic curves, analytic functions, elliptic functions, Weierstrass sigma, zeta and rho-functions, elliptic integrals, projective space, isogenies and the *j*-invariant. The followings days featured talks on fundamental topics of theory, particularly about elliptic curves over the field of rational numbers and finite fields. These include discussions on the torsion subgroup and Nagell-Lutz theorem, descent, heights and the Mordell-Weil Theorem, and the counting of points on an elliptic curve over a finite field. There were also lectures on applications such as the discrete logarithm problem and elliptic curve cryptography. Current research problems were also introduced, including questions about the L-function of an

elliptic curve, congruent numbers and images of Galois representations. The lecturers provided exercises for the participants which helped motivate the ideas discussed throughout the courses. The last session was devoted to a tutorial on the use of the computer algebra system PARI/GP, with examples and computational exercises related to lectures.



The school also provided a venue for discussions and exchange, both formal and informal, between lecturers and participants and between participants, who came from diverse backgrounds and cultures.

Lecturers were given by 8 mathematicians (1 woman and 7 men) from France (1), Italy (1), Canada (1) and the Philippines (5). The 40 participants (including 9 women) came from several countries: Austria (1), India (1), Indonesia (3), Malaysia (1), Philippines (28) and Vietnam (7). Among these were 11 foreign participants who came with complete funding support from the school organizers. The lecturers considered this diversity of backgrounds in determining the content, flow and pace of their lectures.



The school was held in a medium-sized room on the 3rd floor of annex building of the Institute of Mathematics. The room was equipped with a wall-length blackboard, LCD projector and a projection screen. There was also a sound system with microphone and speaker, although its use was not necessary for the lecturers with booming voices. Coffee, snacks and lunch were served in an adjacent room. Another room with office desks and blackboards were made available for the use of the lecturers. Next to it was a designated prayer room for the Muslim participants. There was intermittent wi-fi internet access on the 3rd floor of the building, but a stronger and steadier connection was provided inside the lecture room.

After discussion with the scientific committee, Francesco Pappalardi and Fidel Nemenzo decided to convert parts of their final lectures into sessions to allow some participants to present their research works. Seven (7) participants volunteered for these sessions.

The three lecturers from overseas and almost all participants who were not from the host university were provided accommodation at the NISMED Hostel, the guest house of the National Institute for the Science and Mathematics Education, which is short walk from the school venue. At the NISMED Hostel, participants and lecturers took their breakfast together – an opportunity to interact informally outside the school venue. In the evenings, they had the option of walking to the other side of the campus where a variety of cafeterias offered meals at student prices, or to take a cab to any of the many restaurants in the

nearby areas outside the campus. Two members of the organizing committee were billeted at the NISMED Hostel and were responsible for attending to various concerns of the other participants.

The SEAMS School Manila 2017 commenced on 17 July with a short opening program with UPD Vice-Chancellor for R&D Fidel Nemenzo (member of the SEAMS School Scientific Committee) and Dean Jose Maria Balmaceda of the College of Science giving the welcome remarks in behalf of the host university. They both recounted some of their experiences as lead organizers of the inaugural SEAMS School (on the Applications of Algebra and Analysis) held in Manila in April 2011. A brief message was given by Michel Waldschmidt, representing CIMPA. Jerome Dimabayao (member, SEAMS School Scientific Committee) introduced the lecturers and the participants. The 20-minute opening program was followed by a short coffee break, preparing the participants for the first lecture of the SEAMS School by Dr Dimabayao.

Activities were organized for participants and lecturers on Saturday (22 July). They visited the Pinto Art Museum in Antipolo and got to see some local artworks. Then they had lunch at the Balaw-balaw restaurant and art gallery in Angono- a lakeside town outside the city- where the participants experienced eating local exotic foods. They were then toured inside the Calinawan Cave and made a nature trip to the Daranak Falls, both in Tanay, Rizal. The following day, Sunday (23 July), was a free day for all. This allowed some participants to bond amongst themselves by studying together and walking around the campus.

The final activity of the SEAMS School was the closing program. School lecturers, participants and some faculty members of the Institute of Mathematics enjoyed food and drinks sponsored by the Institute. Representatives from each participating country shared their impressions and experiences about their stay in the Philippines and their participation in the school. They were all happy to learn about elliptic curves and be able make new friends.

The organizers wish to express their deep gratitude to the following organizations for their assistance and generous support to the school and its objectives:

- Centre International de Mathématiques Pures et Appliquées (CIMPA)
- Southeast Asian Mathematical Society (SEAMS)
- Office of International Linkages, Office of the Vice-President for Academic Affairs, University of the Philippines
- Office of the Vice-Chancellor for Research and Development, UP Diliman

- Office of the Chancellor, UP Diliman
- Number Theory Foundation
- Mathematical Society of the Philippines
- Institute of Mathematics, University of the Philippines Diliman

School websites:

1. **Institute of Mathematics, UP Diliman:** http://math.upd.edu.ph/seamsschoolmanila2017/
2. **Southeast Asian Mathematical Society:** http://seams.maths.web.id/current-schools
3. **Roman Number Theory Association:** http://www.rnta.eu/manila2017/

Lecturers:

The lectures at the SEAMS School 2017 Manila were given by:

1. Jared Guissmo Asuncion (Philippines) Institut National de Recherche en Informatique et en Automatique Bourdeaux, France	2. Julius Basilla (Philippines) Institute of Mathematics UP Diliman
3. Richell Celeste (Philippines) Institute of Mathematics UP Diliman	4. Jerome Dimabayao (Philippines) Institute of Mathematics UP Diliman
5. Claude Levesque (Canada) Département de mathématiques et statistique Université Laval	6. Fidel Nemenzo (Philippines) Institute of Mathematics UP Diliman
7. Francesco Pappalardi (Italy) Dipartimento di Matematica e Fisica Università degli Studi Roma Tre	8. Michel Waldschmidt (France) Faculté de Mathématiques Université Pierre et Marie Curie (Paris 6)

Participants (40):

Name	Country	Affiliation
Jose Capco	Austria	Johannes Kepler University
Satinder Pal Singh Sandhu	India	Thapar University
Rian Kurnia	Indonesia	Bogor Agricultural University
Siti Zahidah	Indonesia	Universitas Airlangga
Irmatul Hasanah	Indonesia	Universitas Islam Negeri Syarif Hidayatullah
Siti Noor Farwina	Malaysia	Universiti Sains Malaysia
Cynthia Aba	Philippines	Ateneo de Manila University
Janus Aban	Philippines	University of Sto. Tomas
Carlo Francisco Adajar	Philippines	UP Diliman
Jeffrey Alvarina	Philippines	UP Diliman
Eric Anthony Arances	Philippines	UP Diliman
Joy Ascano	Philippines	UP Baguio
Ron Allan Baran	Philippines	UP Baguio
Rowena Alma Betty	Philippines	UP Diliman
Jonathan Caalim	Philippines	UP Diliman
Clarisson Rizie Canlubo	Philippines	UP Diliman
Gari Lincoln Chua	Philippines	UP Diliman
Raiza Corpuz	Philippines	UP Diliman
John Oliver Doctor	Philippines	UP Diliman
Bryan Ceasar Felipe	Philippines	Ateneo de Manila University
Junmar Gentuya	Philippines	UP Diliman
Russelle Guadalupe	Philippines	UP Diliman
Anton Hilado	Philippines	UP Diliman
Fred Kintanar	Philippines	
Joshua Mengorio	Philippines	Polytechnic University of the Philippines Manila
Little Hermie Monterde	Philippines	UP Diliman
Prince Allan Pelayo	Philippines	UP Diliman
Charles Repizo	Philippines	UP Los Banos
Terence Teh	Philippines	UP Diliman
Mark Tomenes	Philippines	Ateneo de Manila University
Vonn Kee Wong	Philippines	UP Diliman
Daniel Young	Philippines	UP Diliman
Aliw-iw Zambrano	Philippines	Ateneo de Manila University
Thanh Nguyen Vanh	Vietnam	Ho Chi Minh University of Technology
Ngoc Ky Nguyen	Vietnam	University of Technology, VNU-HCM
Tuan Nguyen Anh	Vietnam	University of Science, Ho Chi Minh City
Hoang Nguyen Khanh Huy	Vietnam	Dong Nai University
Khai Hanh Tang	Vietnam	University of Science, Ho Chi Minh City
Tran Ngo	Vietnam	Saigon Technology University
Thi My Le Nguyen	Vietnam	Dong Nai University

Scientific Program:

A. Basic Theory of Elliptic Curves (*Jerome Dimabayao*)
A1. Elliptic curves over an arbitrary field
A2. Weierstrass equations
A3. Projective space and the point at infinity
A4. The group law
A5. Isogenies
A6. The *j*-invariant

B. Elliptic Curves over Q and Number Fields (*Francesco Pappalardi*)
B1. The torsion subgroup and the Nagell-Lutz Theorem
B2. Descent and the weak Mordell-Weil Theorem
B3. The theory of heights
B4. The Mordell-Weil Theorem
B5. The Height Pairing

C. Elliptic Curves over Finite Fields and Applications (*Julius Basilla*)
C1. The discrete logarithm problem and application to elliptic curves
C2. Counting the number of points on an elliptic curve over a finite field
C3. Some algorithms for solving ECDLP
C4. An introduction to elliptic curve cryptography

D. L-functions and Elliptic Curves (*Richell Celeste*)
D1. L-functions
D2. Modular forms
D3. L-function of a modular form
D4. L-function of an elliptic curve
D5. The Birch and Swinnerton-Dyer Conjecture

E. Congruent Numbers (*Fidel Nemenzo*)
E1. Pythagorean triples and rational triangles
E2. Congruent number elliptic curves
E3. Fermat's infinite descent
E4. Tunnel's Theorem

F. Transcendence and Elliptic Functions (*Michel Waldschmidt*)
F1. Analytic functions: infinite products, order of an entire function, Schwarz Lemma.
F2. Analytic theory of elliptic functions: Weierstrass sigma, zeta, $\wp$ functions; elliptic integrals.
F3. Schneider-Lang criterion and consequences: Hermite-Lindemann, Gel'fond-Schneider; transcendence theorems of Schneider.
F4. Linear independence of periods: theorems of Baker, Coates, Masser.
F5. Algebraic independence of periods: theorems of Chudnovski, Nesterenko.

G. Galois Representations of Elliptic Curves (*Jerome Dimabayao*)
G1. Introduction to Galois representations: the *n*th cyclotomic character
G2. Galois action on torsion points of elliptic curves
G3. The Galois representation theorem for elliptic curves

H. Tutorial on the use of PARI for elliptic curve computations (*Jared Asuncion*)

School Schedule: (17 – 21 July 2017)

	Monday	Tuesday	Wednesday	Thursday	Friday
	17-Jul	**18-Jul**	**19-Jul**	**20-Jul**	**21-Jul**
9:00-9:30	Registration / Opening				
9:30-11:30	Elliptic curves over an arbitrary field (JD)	Projective space, the point at infinity and the group law (JD)	Descent and the weak Mordell-Weil Theorem (FP)	The Height Pairing/ Fermat's infinite descent (FP)	Binary quadratic forms and quadratic fields (CL)
11:30-13:00	Lunch Break				
13:00-15:00	Analytic functions: infinite products, order of an entire function, Schwarz Lemma. (MW)	Isogenies and the *j*-invariant (JD)	Counting points on an elliptic curve over a finite field (JB)	The discrete logarithm problem on elliptic curves (JB)	Elliptic curves and quadratic fields (CL)
15:00-15:30	Break				
16:00-17:30	Analytic theory of elliptic functions: Weierstrass sigma, zeta, ρ-functions; elliptic integrals. (MW)		The torsion subgroup and the Nagell-Lutz Theorem (FP)	Short presentations by some participants (1)	An introduction to elliptic curve cryptography (JB)	L-function of an elliptic curve (RC)
18:30-21:00				School Dinner		

Short presentations (1) were given by:

1. Raiza Corpuz : An infinite family of elliptic curves from complex quadrilaterals
2. Carlo Francisco Adajar: On Odd Near-Perfect and Deficient-Perfect Numbers
3. Russelle Guadalupe: *p*-adic construction of elliptic curves of given order
4. Gari Lincoln Chua: An Eigenvector Method for Solving the Three-Coloring Problem

School Schedule: (24 – 25 July 2017)

<table>
<tr><td></td><td>Monday</td><td>Tuesday</td></tr>
<tr><td></td><td>24-Jul</td><td>25-Jul</td></tr>
<tr><td>9:00-9:30</td><td></td><td></td></tr>
<tr><td>9:30-11:30</td><td>The Birch and Swinnerton-Dyer Conjecture (RC)</td><td>Galois representations of elliptic curves (JD)</td></tr>
<tr><td>11:30-13:00</td><td colspan="2">Lunch Break</td></tr>
<tr><td>13:00-15:00</td><td>Congruent number elliptic curves and Tunnell’s Theorem 1 (FN)</td><td rowspan="4">Computations on elliptic curves using PARI: A Tutorial (JA)</td></tr>
<tr><td>15:00-15:30</td><td>Break</td></tr>
<tr><td>15:30-16:00</td><td rowspan="2">Congruent number elliptic curves and Tunnell’s Theorem 2 (FN)</td></tr>
<tr><td>16:00-16:30</td></tr>
<tr><td>16:30-17:30</td><td rowspan="2">Short presentations by some participants (2)</td><td rowspan="2">Closing program</td></tr>
<tr><td>16:00-17:30</td></tr>
</table>

Short presentations (2) were given by:

1. Tang Khai Hanh: LPS Ramanujan Graphs
2. Anton Hilado: Algebraic geometry in number theory
3. Daniel Young: Construction of Galois extensions of **Q** using elliptic curves