Znanstveni centar izvrsnosti QuantiXLie

Element 7: Teorija brojeva, eliptičke krivulje i modularne forme

Znanstveni centar izvrsnosti
za kvantne i kompleksne sustave te
reprezentacije Liejevih algebri

Projekt KK.01.1.1.01.0004

Projekt je sufinancirala Europska unija iz Europskog fonda za regionalni razvoj. Sadržaj ovog seminara isključiva je odgovornost Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu te ne predstavlja nužno stajalište Europske unije.

Europska unija
Zajedno do fondova EU

EUROPSKI STRUKTURNI
I INVESTICIJSKI FONDOVI

Operativni program
KONKURENTNOST
I KOHEZIJA

EUROPSKA UNIJA
Europski fond za regionalni razvoj

Članovi:

Andrej Dujella, redoviti profesor

Zrinka Franušić, izvanredni profesor

Matija Kazalicki, izvanredni profesor

Filip Najman, izvanredni profesor

Tomislav Pejković, docent

Vinko Petričević, poslijedoktorand (ZCI)

Tomislav Gužvić, doktorand (ZCI)

Ivan Krijan, doktorand

Antonela Trbović, doktorand (ZCI)

Borna Vukorepa, doktorand (ZCI)

Konferencija: Torsion groups and Galois representations of elliptic curves, Zagreb, 25.–29.6.2018.

Glavni organizator: Filip Najman

50 sudionika, 29 predavanja

Pozvani predavači:
Abbey Bourdon (Wake Forest), Peter Bruin (Leiden), Maarten Derickx (Bayreuth), Vladimir Dokchitser (King's College London), Tom Fisher (Cambridge), Enrique Gonzalez-Jimenez (Madrid), Daeyeol Jeon (Kongju), Alvaro Lozano-Robledo (University of Connecticut), Loic Merel (Paris Jussieu), Pierre Parent (Bordeaux), Marusia Rebolledo (Clermont-Ferrand), Rene Schoof (Rome, Tor Vergata), Peter Stevenhagen (Leiden), Michael Stoll (Bayreuth), Andrew Sutherland (MIT), David Zureick-Brown (Emory).

TORSION GROUPS AND GALOIS REPRESENTATIONS OF ELLIPTIC CURVES

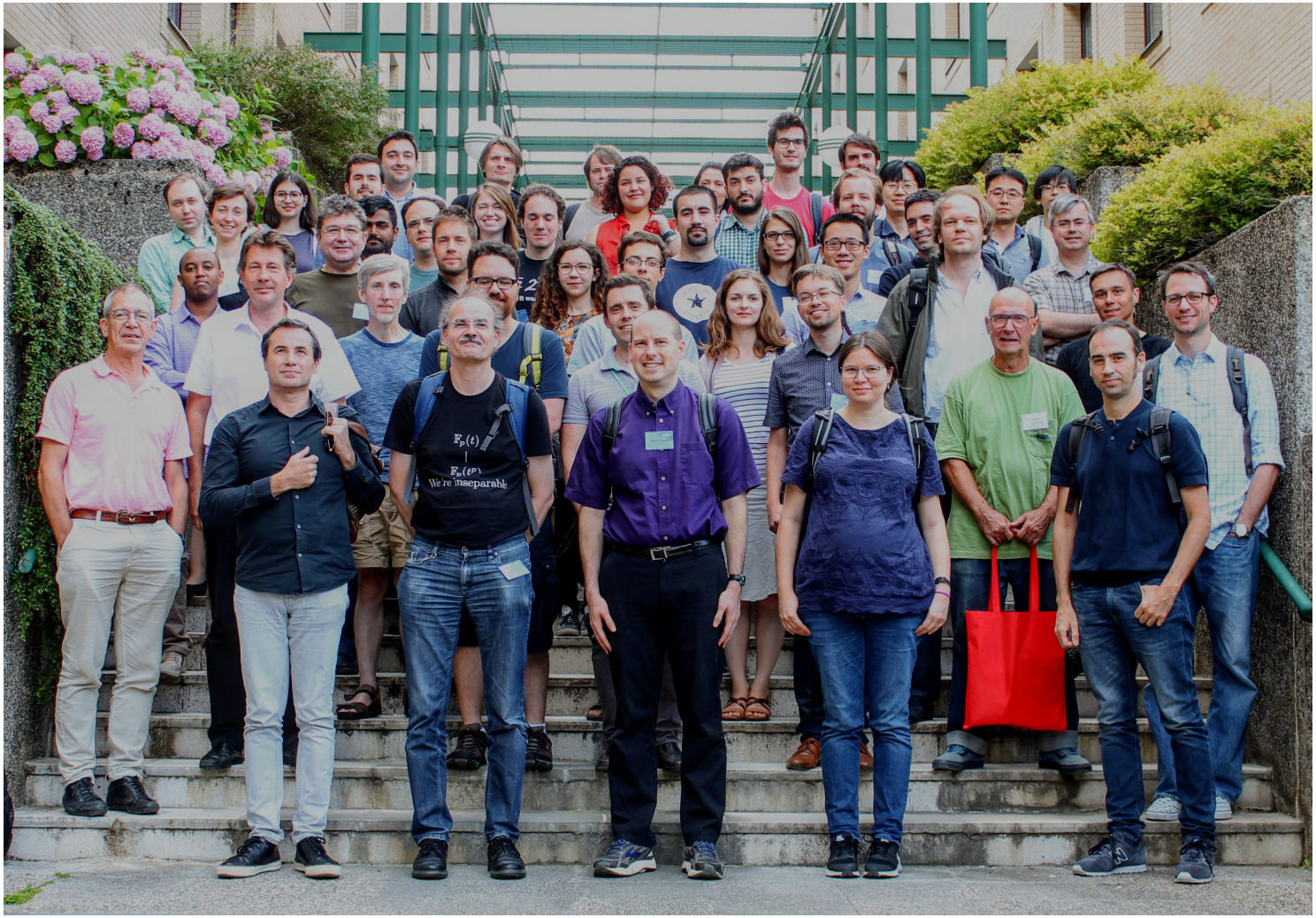
UNIVERSITY OF ZAGREB, JUNE 25-29, 2018

ORGANIZERS

- Andrej Dujella
- Matija Kazalicki
- Filip Najman

INVITED SPEAKERS

- Abbey Bourdon
- Peter Bruin
- Pete Clark
- Maarten Derickx
- Vladimir Dokchitser
- Tom Fisher
- Enrique Gonzalez-Jimenez
- Daeyeol Jeon
- Alvaro Lozano-Robledo
- Loic Merel
- Pierre Parent
- Marusia Rebolledo
- Rene Schoof
- Peter Stevenhagen
- Michael Stoll
- Andrew Sutherland
- David Zureick-Brown


$F_p(t)$
$F_n(t^p)$
We're inseparable

Radionica: Lectures on computational aspects of algebraic geometry, Zagreb, 13.–17.6.2018.

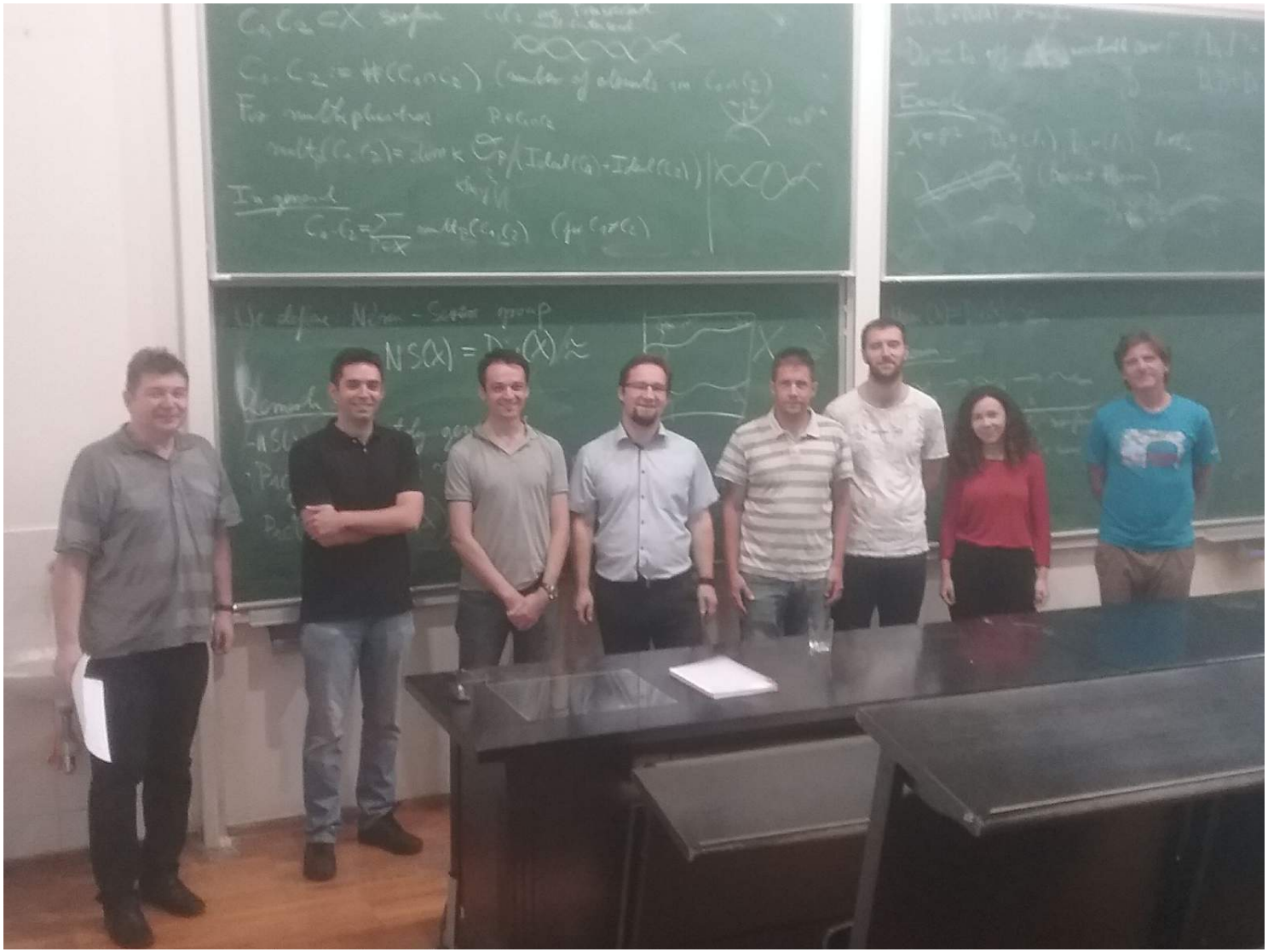
Glavni organizator: Matija Kazalicki

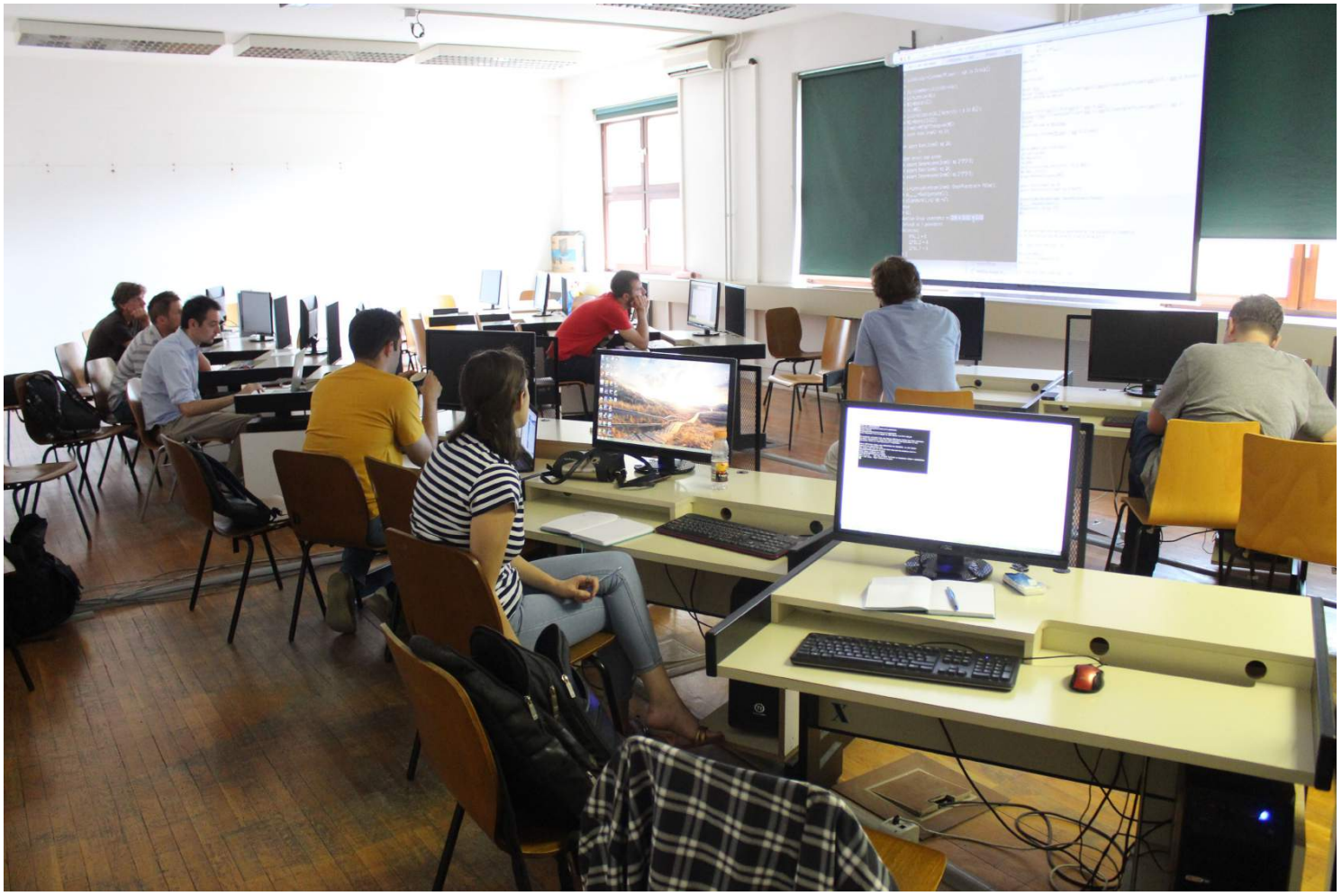
Predavači:

Zvonimir Bujanović (Zagreb): Mini course on GPU programming and applications

Dino Festi (Mainz): Computing the Picard lattice of a genus two $K3$ surface

Bartosz Naskrecki (Poznan): Mini course on Elliptic surfaces





Eliptičke krivulje:

- važno i aktualno područje istraživanja koje koristi metode iz teorije brojeva, algebarske geometrije i kompleksne analize, a ima i primjene u kriptografiji

- Mordell-Weilov teorem: skup racionalnih točaka na eliptičkoj krivulji konačno generirana Abelova grupa, što znači da je izomorfna direktnom produktu torzijske grupe i r (rang) kopija cijelih brojeva.

- **Najman** i njegovi doktorski studenti **Gužvić**, **Krijan**, **Trbović**, **Vukorepa**: određivanje svih mogućih torzijskih grupa na eliptičkim krivuljama nad poljima algebarskih brojeva malog stupnja, svojstava eliptičkih krivulja sa zadanim torzijskim grupama, te svojstva krivulja s izogenijama velikog stupnja.

Modularne forme:

- Analitičke funkcije na gornjoj poluravnini koje su invarijantne s obzirom na djelovanje modularne grupe, te zadovoljavaju još neka dodatna svojstva.

- **Kazalicki:** Veze između aritmetičkih svojstava Fourierovih koeficijenata modularnih formi i aritmetičke geometrije, posebice vezano uz Atkin i Swinnerton-Dyerove kongruencije.

- Modularne forme su bitne za razumijevanje modularnih krivulja, koje su vrlo korisne kod proučavanja eliptičkih krivulja sa zadanim torzijskim grupama nad poljima algebarskih brojeva (**Kazalicki**, **Najman**, **Krijan**, **Trbović**).

Diofantove m-torke:

- skupovi cijelih ili racionalnih brojeva sa svojstvom da produkt svaka dva među njima uvećan za 1 daje kvadrat

- Koliko veliki mogu biti ovi skupovi? Nema cjelobrojnih Diofantovih petorki. Postoji beskonačno mnogo racionalnih Diofantovih šestorki. Postoji li racionalna Diofantova sedmorka?

- **Kazalicki**, **Petričević**, **Dujella**:
$\{\frac{14212}{15435}, \frac{6768}{665}, \frac{2392}{5985}, \frac{2044}{95}, \frac{270}{133}, \frac{46300}{31329}, \frac{26600}{114921}\}$
je "skoro sedmorka" (samo jedan uvjet nedostaje)

- primjene na konstrukciju krivulja velikog ranga

- **Franušić**: analogan problem u poljima algebarskih brojeva malog stupnja

Diofantske aproksimacije:

- Koliko se dobro može iracionalni broj aproksimirati s racionalnim?
$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$ ima beskonačno mnogo rješenja

- Problem separacije korijena polinoma: koliko bliska mogu biti dva različita korijena polinoma P s cjelobrojnim koeficijentima (u ovisnosti o stupnju n i maksimumu apsolutnih vrijednosti koeficijenata $H(P)$)?
$|\alpha - \beta| > c_n H(P)^{-n+1}$ (Mahler)

- Je li eksponent $-n+1$ u Mahlerovom teoremu najbolji mogući?

- Varijante problema: ireducibilni polinomi, normirani polinomi, apsolutna separacija, separacija u p-adskoj normi, ... (**Pejković**, **Dujella**)