אוניברסיטת בן-גוריון בנגב

# המחלקה למתמטיקה

סמסטר 19—2018—א

**שם הקורס** עקומים אליפטיים ותבניות מודולריות

**מספר קורס** 201.2.5291

**עמוד הקורס ברשת**
https://math.bgu.ac.il//he/fall2019/courses/elliptic-curves-and-modular-forms

**מרצה אחראי** ד"ר דניאל דיסני, <disegni@bgu.ac.il>, חדר 108

**שעות קבלה** https://math.bgu.ac.il/he/hours

## תקציר

## דרישות והרכב ציון הקורס[1]

[1] דרישות הקורס יכולות להשתנות במהלך השבועיים הראשונים של הסמסטר, ויש לשים לב להודעות באתר הקורס

# ELLIPTIC CURVES AND MODULAR FORMS (BGU, FALL 2018)
# COURSE ANNOUNCEMENT – 201-2-5291

INSTRUCTOR: DR. DANIEL DISEGNI
FALL 2018

**Elliptic curves** are the first really interesting examples of algebraic curves. They can be defined by cubic equations $F(x,y) = 0$ in two variables. The solution set of such an equation in the complex numbers is a torus, the first really interesting example of a *Riemann surface* (a surface with a notion of holomorphic functions on it, which locally looks like $\mathbf{C}$).[1] If the coefficients of $F$ are integers, one can study the set of solutions in other rings ($\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{F}_p$): this is a central open problem in number theory, with important application to cryptography.

**Modular forms** are special holomorphic forms $f(z)$ of one variable which are highly symmetric: they are almost invariant under an action of the group $\mathrm{SL}_2(\mathbf{Z})$. They are of central interest in number theory and appear frequently in many other areas of mathematics and theoretical physics.

The best (known or partial or conjectured) solutions to the following problems all rely on modular forms and their generalisations:

(1) which integers are sums of four squares, and in how many ways? (Lagrange, 1770; Jacobi, 1829)
(2) does the equation $a^n + b^n = c^n$ have any nontrivial integer solutions for $n \geq 3$? (Wiles, 1993)
(3) what is the densest possible packing of $n$-spheres in $\mathbf{R}^n$? (Viazovska et al., 2016)
(4) let $E : F(x,y) = 0$ be an elliptic curve defined by an $F$ with integer coefficients. Let $E(K)$ be the set of its solutions in the field $K$.
   (a) what is the relation among the numbers $|E(\mathbf{F}_p)|$ as $p$ varies among the primes? (Wiles et al., ∼2000)
   (b) how to construct rational solutions in $E(\mathbf{Q})$? (Heegner, 1952)
(5) which vector spaces have actions by huge bizarre finite simple groups? (Borcherds, 2000)

Some of the main themes of the course will be:

(a) the wonders of holomorphic functions with special symmetry;
(b) how to construct abstract spaces (the space on which a multivalued function is a function; the space of all lattices) and how to describe them concretely;
(c) fun applications to arithmetic and elsewhere.

**Who this course is for**
Advanced undergraduate and beginning graduate students.

**Recommended references**
J. Milne, *Elliptic curves*, online notes.
J.-P. Serre, *A course in Arithmetic*, Springer.
D. Zagier, in *The 1-2-3 of modular forms*, Springer

[1] The discrepancy 'curve' / 'surface' is due to: $\dim_{\mathbf{C}} \mathbf{C} = 1$, $\dim_{\mathbf{R}} \mathbf{C} = 2$.

**Plan**

(1) Lattices. Doubly periodic functions.
(2) Riemann surfaces: definition and examples (Riemann sphere, roots, logarithms).
(3) Riemann surfaces: Euler characteristic, genus, Hurwitz formula. Riemann–Roch theorem (statement)
(4) Complex tori and elliptic curves.
(5) Morphisms between elliptic curves. The group law. Arithmetic of elliptic curves (a glimpse: Mordell's theorem, $L$-function, the Birch and Swinneton-Dyer conjecture).
(6) The group $\mathrm{SL}_2(\mathbf{Z})$. The space of all lattices. The trefoil knot.
(7) Modular forms for $\mathrm{SL}_2(\mathbf{Z})$: finite-dimensionality. Eisenstein series.
(8) Theta series. Four squares. Even unimodular lattices and sphere packing in dimension 8.
(9) Hecke operators. 'Reminders' on the Riemann zeta function. $L$-functions.
(10) The Ramanujan conjecture. Expander graphs. The $j$-invariant. Moonshine.
(11) Modular curves and their compactification.
(12) Complex multiplication.

**Practical details**

When and where: room -101, Tuesdays 12-14 and Wednesdays 10-12.

The course will be taught in English. Students will be *encouraged* but *not obliged* to submit their written work in English.

The final grade will be the best of: 40% homework + 60% final exam, or 60% homework + 40% final exam.

*E-mail address*: daniel.disegni@gmail.com

אוניברסיטת בן-גוריון בנגב

## נושאי לימוד

1. סריגים, פונקציות בעלות מחזור כפול.
2. משטחי רימן: הגדרה ודוגמאות (הספירה של רימן, שורשים, לוגריתמים).
3. משטחי רימן: מציין אוילר, גנוס, נוסחת הורביץ, משפט רימן-רוך (ללא הוכחה).
4. טורוסים מרוכבים ועקומים אליפטיים.
5. העתקות בין עקומים אליפטיים, חוק החבורה, אריתמטיקה של עקומים אליפטיים (הצצה: משפט מורדל, פונקציות L, ההשערה של בירץ' וסווינרטון-דייר).
6. החבורה $SL(2,Z)$, מרחב כל הסריגים, קשר התלתן.
7. תבניות מודולריות על $SL(2,Z)$: סופיות המימד, טורי אייזנשטיין.
8. טורי טיתא, סכום של ארבעה ריבועים, סריגים אונימודולריים זוגיים ואריזות כדורים במימד 8.
9. אופרטורי הקה, "תזכורת" על פונקצית זיתא של רימן, פונקציות L מודולריות של עקומים אליפטיים (בלי הוכחה).
10. השערת רמנוג'ן, גרפים מרחיבים, אינווריאנטת j, מונשין.
11. עקומים מודולריים והקומפקטיפיקציה שלהם.
12. מכפלה מרוכבת.