עקומים אליפטיים:

אנחנו מתעניינים בעקומים במישור הפרויקטיבי המרוכב. עקום הוא פתרון של משוואה פולינומיאלית $f(x,y)=0$, כאשר f פולינום ב-2 משתנים. המשוואה הזו נתונה בקורדינטות x,y, שלהן קוראים **הקורדינטות האפיניות** של המישור. הן מאפשרות לתאר רק נק' שאינן על הישר האינסופי. כדי לקבל את הנק' בישר האינסופי צריך לעבור ל**קורדינטות הומוגניות**, שיסומנו $(x:y:z)$, כשה-":" מתארות את העובדה שאנו מתעניינים רק ביחסים בין הנק'. בקורדינטות אלה, הישר באינסוף מתואר ע"י המשוואה $z=0$.

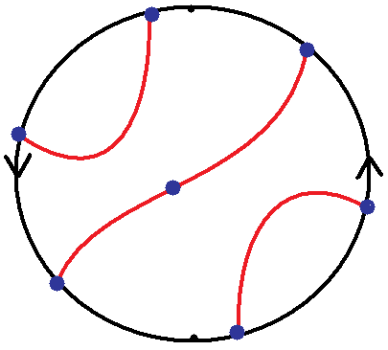
כל עקומה שנתונה ע"י משוואה בקורדינטות אפיניות ניתן לתרגם למשוואה הומוגנית בקורדינטות ההומוגניות. התרגום נעשה כך: אם המשוואה היא מדרגה d, אז לכל מונום $x^i y^j$ שמופיע במשוואה נכפול אותו ב-z^{d-i-j} כך שנקבל מונום מדרגה d בדיוק. גיאומטרית, זה אומר שהוספנו לעקומה שלנו את הפתרונות באינסוף. כדי לתרגם את המשוואה למשוואה אפינית, עושים את הפעולה ההפוכה: מציבים $z=1$. המילון הזה בין הקורדינטות נותן שקילות בין עקומות אפיניות ועקומות פרויקטיביות שלא מכילות את הישר באינסוף.

העקומים שנדבר עליהן היום הם עקומים מדרגה 3. שלא כמו במקרה של קוניקות (עקומות מדרגה 2), יש הרבה עקומות מדרגה 3 שלא עוברות אחת לשנייה ע"י העתקה פרויקטיבית. בשיחה הזו, ננסה למיין את כל העקומות מדרגה 3 שהן חלקות, כלומר כאלה שבכל נק' מקורבות טוב ע"י ישר.
עקום חלק מדרגה 3 נקרא **עקום אליפטי**. הקשר לאליפסות היסטורי ולא מעניין אותנו כרגע.

<u>מיון של עקומים אליפטיים:</u>

נתבונן בעקום אליפטי כללי $ax^3+bx^2y++cxy^2+dy^3+ex^2+fxy+gy^2+hx+iy+j=0$.
משוואה כזו תלויה ב-10 פרמטרים, אבל בעצם רק ב-9 כי אפשר לכפול הכול בקבוע. העתקה פרויקטיבית נקבעת ע"י 4 נק', לכן יש לנו 8 דרגות חופש בקביעה של העתקה פרויקטיבית. לכן, נצפה שעד כדי העתקה פרויקטיבית תהיה לנו משפחה 1-פרמטרית של עקומות מדרגה 3.

השלב הראשון בהתעללות במשוואה יהיה לנסות להביא למינימום את מספר המונומים מדרגה 3. לשם כך נרצה לדאוג שהעקום שלנו יחתוך את הישר באינסוף בדיוק בנק' אחת. נק' כזו חייבת להיות נק' פיתול של העקום, כלומר נק' שבו הכיוון של העקומיות מתהפך. נרצה לשלוח נק' כזו לישר האינסופי, ונטען כי תמיד נק' כזו קיימת:



אז למה על עקום מדרגה 3 תמיד יש נק' פיתול? בואו נסתכל על העקום במישור הפרויקטיבי, ונסה להבין איפה הכיוון של העקמומיות שלו מתהפך. זה יכול לקרות ב-2 סוגים של נק': או כאשר חותכים את הישר באינסוף ואז יוצאים מצד שני והאוריינטציה מתהפכת, או בנק' פיתול. יש מס' אי זוגי של חיתוכים עם הישר באינסוף, אם סופרים עם ריבוי (קל לבדוק שבכל אחד מהמקרים זה תורם מספר אי זוגי של היפוכי כיוון לעקמומיות). לכן, בגלל שבסוף הכיוון של העקמומיות חוזר למקום המקורי שלו, חייבת להיות גם נק' פיתול.

עכשיו כדי להיפתר מהגורמים מחזקות גבוהות, נבחר נק' פיתול של העקום, ונשלח אותה לנק' $(0:1:0)$, כך שהמשיק בנק' יעבור לישר האינסופי. אז כשנציב במשוואה $z=0$, נקבל פולינום מדרגה 3 הומוגני ב-x,y שמתאפס רק בנק' $(0:1:0)$, לכן הוא חייב להיות כפולה של x^3. כעת המשוואה שלנו היא

מהצורה: $ax^3+ex^2+fxy+gy^2+hx+iy+j=0$, או, אם נשים בצד אחד את כל המונומים שמכילים את y ונעשה הומוגניזציה, משוואה
מהצירה $gy^2z+fxyz+iyz^2=ax^3+ex^2z+hxz^2+jz^3$

טענה: במשוואה שקיבלנו לא ייתכן כי $g=0$.

הסיבה היא שבמקרה כזה, העקום יוצא לא חלק. כדי לראות את זה, בואו נסתכל על העקום קרוב מאוד לנק' (0:1:0). נבחר קורדינטות אפיניות לנק', למשל ע"י הצבת $y=1$, ונקבל:
$gz+fxz+iyz^2=ax^3+ex^2z+hxz^2+jz^3$. אם $g=0$, המשוואה שיוצאת מכילה רק גורמים מסדר 2 ומעלה. החלק מדרגה 3 זניח ביחס לחלק מדרגה 2 קרוב לנק' ולכן נזניח אותו ונקבל:
$fxz+O(x^3+y^3)=0$. לכן, שני ישרי הצירים משיקים לעקום בנק' ומכיוון ויש שני משיקים שונים העקום לא חלק.

מכאן שבעקום אליפטי $g\neq 0$ וניתן להניח כי הוא שווה ל-1 ע"י זה שנכפול את המשוואה בקבוע.
כעת, ע"י השלמה לריבוע ניתן להיפתר גם מ- xy, y ולקבל משוואה מהצורה:
$y^2=f(x)$, כאשר $f(x)=ax^3+bx^2+cx+d$ פולינום מדרגה 3. לא ייתכן כי $a=0$, כי העקום יצא מדרגה 3. לכן ניתן ע"י הזזה ב- x להיפתר גם מ- x^2. ניתן גם לדאוג ש- $a=1$, ע"י זה שנכפול את x, y ב- a^{-1} ונצמצם. לבסוף, ניתן לחסל את b ע"י השלמה לחזקה שלישית.

אחרי כל העבודה הזאת, קיבלנו את הצורה הכללית הבאה:

$$y^2=x^3+Ax+B.$$

אבל הבטחנו שתהיה רק דרגת חופש אחת! נכון, זה בגלל שניתן עדיין לעשות הצבה $\begin{matrix} y\leftarrow u^3y \\ x\leftarrow u^2x \end{matrix}$, בלי לפגוע בצורה של המשוואה. לעקומות מהצורה הזו יש כל מיני צורות:
[ציורים!!!].
ניתן לראות שנק' לא חלקה מתקבלת בדיוק כאשר לפולינום שלנו יש שורש כפול. ניתן לרשום כמשוואה במקדמים ע"י כך שנחשב את הדיסקרימיננטה.

מתקיים:

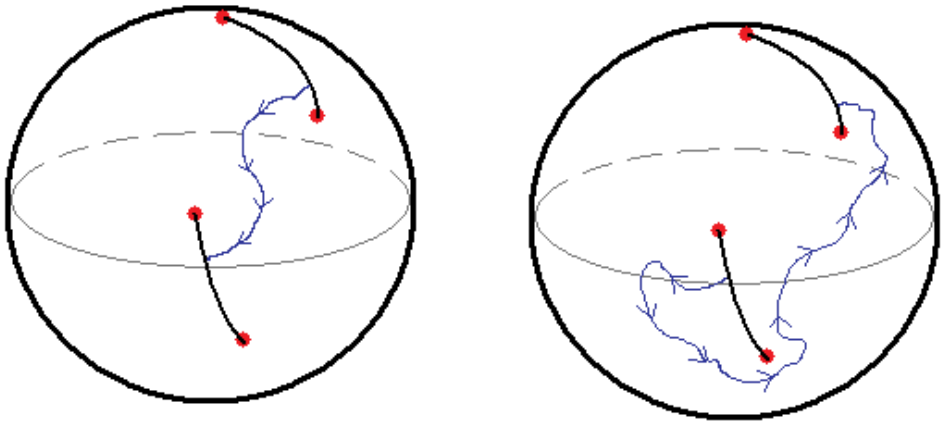
$$\Delta(x^3+Ax+B)=\det\begin{pmatrix}1&0&A&B&0\\0&1&0&A&B\\3&0&A&0&0\\0&3&0&A&0\\0&0&3&0&A\end{pmatrix}=\det\begin{pmatrix}1&0&A&B&0\\0&1&0&A&B\\0&0&-2A&-3B&0\\0&0&0&-2A&-3B\\0&0&3&0&A\end{pmatrix}=$$

$$\det\begin{pmatrix}-2A&-3B&0\\0&-2A&-3B\\3&0&A\end{pmatrix}=4A^3+27B^2.$$

לביטוי הזה קוראים הדיסקרימיננטה של העקום והוא מסומן פשוט ב-Δ. כאשר מבצעים את הטרנספורמציה $\begin{matrix} y \leftarrow u^3 y \\ x \leftarrow u^2 x \end{matrix}$ הוא מתנפח פי u^{-12}. לכן, כדי ליצר פונקציה שמוגדרת בדיוק על עקומים אליפטיים (כלומר, לא שואפת לאינסוף על עקום אליפטי חלק) ותלויה רק בעקום, מגדירים $j(E) = C \cdot \frac{A^3}{\Delta}$ כאשר C קבוע שלא מעניין אותנו כרגע. זה נקרא אינו וריאנט j על שם יעקובי.

<u>עקומים אליפטיים מרוכבים:</u>

מעל למרוכבים, עקום אליפטי הוא משטח דו מימדי. הצורה שלו, מסתבר, היא טורוס.
כדי לראות את זה, נסתכל על הישר המרוכב הפרויקטיבי, ועל המשוואה $y^2 = f(x)$. ניתן "לפתור" אותה ע"י $y = \sqrt{f(x)}$. הבעיה היא שלזה יש כמעט תמיד 2 פתרונות. אם בכל מקום היו בדיוק 2 פתרונות יכולנו פשוט לייצר 2 העתקים של הספרה, אחת לכל פתרות, ולקבל זוג ישרים פרויקטיביים מרוכבים. הבעיה היא שפה יש **נק' הסתעפות**, כלומר נק' כאלה שבהן שני הפתרונות נדבקים לפתרון אחד. כשמקיפים נק' כזו עלולים לקפוץ בין הפתרונות השונים. כדי לפתור את הבעיה, נבצע פעולה שנקראת **חיתוך ענפים** (branch cut). נחלק את הנק' הסתעפות לזוגות ונחבר כל זוג בקו. נחליט, שכאשר חוצים את הקו בספרה אחת, עוברים לספרה השנייה ולהיפך. על המשטח שקיבלנו y הוא כבר פונקציה של הנק' בלבד, ולכן המשטח הזה נראה בדיוק כמו קבוצת הפתרונות למשוואה.
משטח כזה נקרא משטח **רימן**. אצלנו יש 4 נק' הסתעפות, אחת באינסוף ואחת לכל שורש של הפולינום f. לכן, המשטח שנקבל נוצר כך: קח 2 ספרות, תחרוץ בכל אחת 2 חריצים, ותדביק אותן לאורך החריצים. זה בדיוק טורוס!
טורוס אפשר לבנות גם ע"י זה שמזהים צלעות נגדיות של מקבילית. ליצור כזה יש מבנה טבעי של חבורה, כשחיבור הוא לחבר נק' במישור ולהזיז חזרה לתוך המקבילית ע"י הזזות בקודקודי המקבילית. את חוק החבורה הזה אפשר לנסח גם במונחי המשוואה של העקום האליפטי, ובצורה מאוד פשוטה. אנחנו לא נראה את השקילות:



<u>חוק חבורה:</u>

לעקום אליפטי יש תמיד מבנה טבעי של חבורה חילופית. איך מגדירים אותו? באופן הבא:
יהיו $P,Q \in E$ נק' על העקום האליפטי. ניקח את הישר שמחבר אותן, ותהי R נק' החיתוך השלישית שלו עם E. נשקף את R ביחס לציר ה-x, ולנק' שהתקבלה נקרא $P+Q$.
[תמונה!!]
אפשר לנסח את הכלל הזה בצורה פשוטה: סכום 3 נק' הוא 0 אם ורק אם הן על ישר אחד.

מזה נובע ישירות שהנגדי לנק' הוא השיקוף שלה ביחס לציר ה-x ושהנק' באינסוף היא איבר היחידה.

נשאר לבדוק שהכפל הוא אסוציאטיבי, כלומר, ש-$P+(Q+R)=(P+Q)+R$.

לשם הוכחת הטענה הזו נזדקק למשפט אוילר:

משפט (אוילר): יהיו C,C' זוג עקומות מדרגה 3 במישור, לפחות אחת מהן חלקה, הנחתכות ב-9 נק'. כל עקום מדרגה 3 העובר ב-8 מתוך הנק' עובר גם בתשיעית.

הוכחה: נספור מימדים. מרחב הפולינומים מדרגה 3 במישור הוא 10 מימדי. אם נצליח להוכיח כי כל נק' מבין ה-8 מורידה את המימד בדיוק ב-1, נקבל משפחה דו ממדית, ולכן כזו הנפרשת ע"י C,C'. בזה נסיים כי כל צירוף ליניארי שלהם יעבור כמובן בנק' התשיעית.

כדי להראות שכל נק' נוספת מורידה את המימד ב-1, נראה כי בהינתן 8 נק' כלשהן על עקום אליפטי, יש עקום מדרגה 3 שעובר ב-7 ולא בשביעית. ברור שזה גורר את המקרה של פחות נק' (אפשר להוסיף נק' אקראיות).

נסמן ב-r את הנק' השמינית, וב-$p_1,...,p_7$ את שבע הנק' הראשונות
רעיון הוא כמובן להעביר אליפסה דרך 5 נק' וישר דרך 2 נק', שלא יפגשו את הנק' השמינית. הבעיה היא שיכול להיות שיש ישרים שיעברו בנק', וכנ"ל לגבי אליפסות. נוכיח כמה טענות עזר שיקטינו את כמות המקרים שיש לבדוק:

טענה 1: אין 4 נק' בקבוצה על ישר אחד.
הוכחה: אחרת, הישר היה פוגש עקום אליפטי חלק ב-4 נק', בסתירה למשפט ביזו.

טענה 2: אין בין 8 הנק' שבע נק' על אותה אליפסה
הוכחה: אותו הדבר

טענה 3: קיימת $q \in \{p_1,...,p_7\}$ כך שהישר שעובר דרכה ודרך r לא עובר באף נק' נוספת.
הוכחה: מזוגיות, כי אחרת לפי טענה 1 כל שבע הנק' היו מתחלקות לזוגות, לפי הישרים דרך r.

כעת, נניח בלי הגבלת הכלליות כי $q=p_1$. נעביר ישר l דרך p_1, p_2, ואליפסה דרך 5 הנק' הנותרות. ייתכן שהאליפסה עוברת ב-r אבל אז נחליף את p_2 ב-p_3. אם שוב האליפסה עברה ב-r נקבל 2 אליפסות שנחתכות ב-5 נק' ולכן הן חייבות להיות שני זוגות ישרים שנפגשים בישר. מכאן, שיש 3 נק' מבין ה-7 שהן על ישר אחד שאינו עובר ב-r. נעביר דרכן ישר, ואליפסה דרך 4 הנותרות. אם כל אליפסה כזו עוברת ב-r, אז בהכרח יש 3 מה-4 נק' הנותרות שהן על ישר אחד משותף עם r (תרגיל), וזו סתירה לטענה 1.

מכאן שבכל מקרה, נוכל למצוא עקום כרצוננו, והטענה הוכחה.

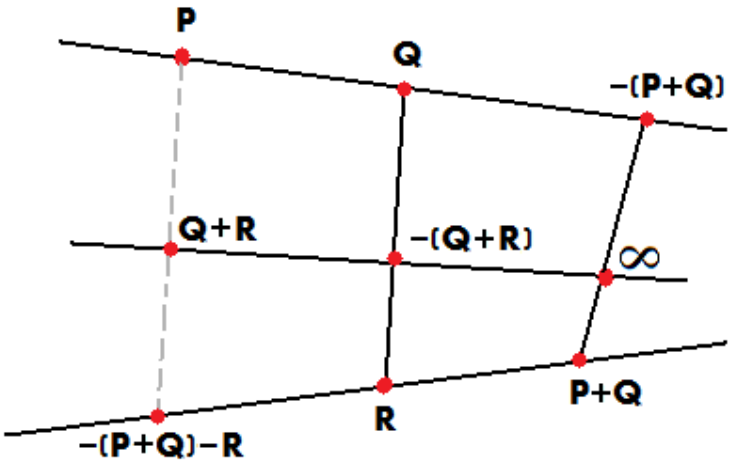
הוכחת אסוציאטיביות החיבור:
זו תוצאה דיי ישירה של משפט אוילר: נתבונן בנק' $\infty, P, Q, -(P+Q), P+Q, R, -R-(P+Q), -(R+Q), R+Q$. כל אחת מהשלשות הבאות נמצאת על ישר אחד:

$[P;Q;-(P+Q)]$

$[P+Q;R;-R-(P+Q)]$.

$[\infty;-(R+Q),(R+Q)]$

עכשיו נחליף תפקידים בין P ו-R, ונקבל עקום נוסף העובר ב-8 מהנק', וגם בנק' $-P-(Q+R)$. לפי משפט אוילר נקבל כי הנק' התשיעיות של כל שלישיית ישרים הן אותה נק', ולכן $-P-(Q+R)=-(P+Q)-R$.
זה כמובן כבר גורר אסוציאטיביות.



כאן אפשר לעצור אם נגמר הזמן!!

<u>מסקנה גיאומטרית יפה:</u>

בעזרת חוק החבורה ניתן להפוך זהויות טפשיות על חיבור לטענות מגניבות בגיאומטריה. למשל:

מה המשמעות הגיאומטרית של הזהות:
$a+b+c+d+e+f=0 \Rightarrow -2(a+b+c+d+e+f)=0$?
כדי לתת לזה משמעות גיאומטרית, נעזר בטענה הבאה:

טענה: 6 נק' על עקום אליפטי מסתכמות ל-0 אם ורק אם הן כולן על אותה הקוניקה.

הוכחה: נוכיח את הכיוון שסכום נק' על אליפסה הוא 0, הכיוון השני ינבע מקשיחות של התמונה.
תהיינה A,B,C,D,E,F 6 נק' על העקום האליפטי, שהן עם אותה אליפסה Λ. נתבונן בנק' $-(A+B),-(C+D),-(E+F)$. נתבונן בעקום שהוא האיחוד של Λ ושל הישר $[-(A+B);-(C+D)]$. זה עקום מדרגה 3 שעובר ב-8 מהנק':
$A,B,C,D,E,F,-(A+B),-(C+D),-(E+F)$. לפי משפט אוילר, העקום עובר גם בנק' $-(E+F)$. מכאן, שהנק' $-(A+B),-(C+D),-(E+F)$ כולן על העקום, התשיעית כלומר בנק' ומכיוון ואף אחת מהן איננה על האליפסה (נשאיר כתרגיל את המקרה המנוון שבו אחת מהן כן!) הן כולן על אותו הישר. לכן סכומן אפס, כמו שרצינו!.

מהו כעת הפירוש של $a+b+c+d+e+f=0 \Rightarrow -2(a+b+c+d+e+f)=0$.
זוהי הטענה הבאה:

טענה: תהיינה A,B,C,D,E,F שש נק' על עקום אליפטי שכולן על אותה האליפסה. נעביר דרך כל אחת מהן משיק לעקום האליפטי וניקח את 6 נק' החיתוך של המשיקים עם העקום. אז כל הנק' שקיבלנו הן על אותה אליפסה.

אתם מוזמנים לחפש עוד דברים נחמדים כאלה בעצמכם.

הערה: הטענה לגבי נק' שהן על אותה אליפסה ניתנת להכללה לחיתוך של עקום אליפטי עם כל עקום. זה יותר קשה ומבוסס על משפט ממש חשוב בגיאומטריה שנקרא **משפט רימן רוך**.

אפשר לעצור כאן אם נגמר הזמן

איברים מסדר סופי:

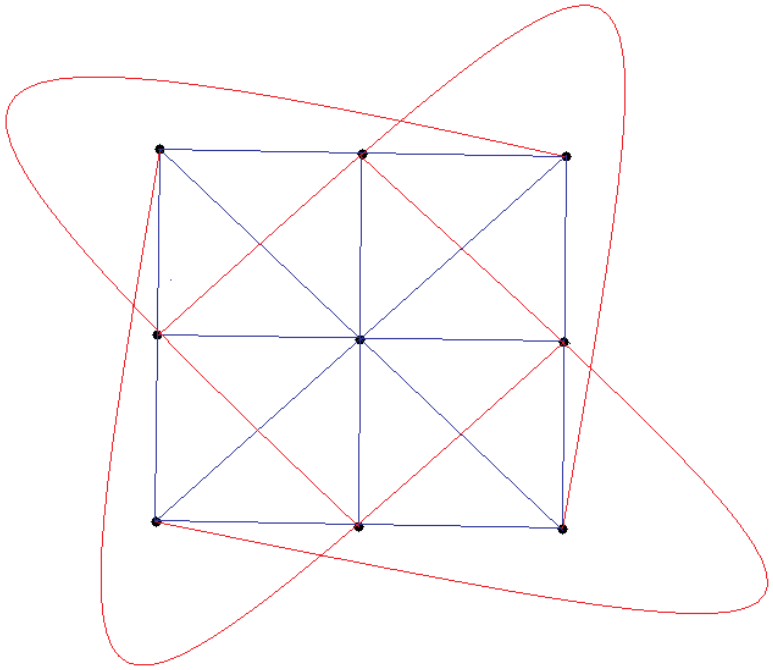
אם יש לנו איבר של חבורה $g \in G$, אז **הסדר** של g הוא המספר הטבעי הקטן ביותר כך ש- $g^n = e$. בחבורה חילופית, קבוצת כל האיברים מסדר נתון זו תת חבורה, שתסומן $G[n]$.

טענה: יהי E עקום אליפטי מעל המספרים המרוכבים. אז $E[n] \cong Z/nZ \oplus Z/nZ$

הוכחה: מעל למרוכבים יש לנו את התיאור של העקום בתור מקבילית שהדביקו לה את הצלעות הנגדיות. זה כמו להסתכל בנק, על המישור המרוכב עד כדי השריג שנפרש ע"י המקבילית, כלומר מעל למרוכבים: $E \cong C/\Lambda$ כאשר Λ השריג שנפרש ע"י המקבילית. על החבורה הזו ברור מהן הנק' מסדר n, זה בדיוק $\frac{1}{n}\Lambda / \Lambda$. בתוך המקבילית יש בדיוק n^2 נציגים לדבר הזה, והם נפרשים ע"י שני ווקטורים פרימיטיביים של השריג $\frac{1}{n}\Lambda$ שיוצרים מקבילית ריקה מנק' שריג נוספות.

זה מאפשר לממש את החבורה $Z/nZ \oplus Z/nZ$ במישור הדו מימדי הפרויקטיבי המרוכב, כך ש-3 נק' הן על ישר אחד בדיוק כשסכומן 0. זה לגמרי לא טריוויאלי לבנות משהו כזה בדרך אחרת...
גם מעל R זה יכול לעבוד אם מצליחים למצוא עקום אליפטי עם איברים מסדר נתון שהם ממשיים. זה בפני עצמו לא טריוויאלי לביצוע.

לדוגמא, ניתן לממש במרוכבים תמונה כזו של משחק סט:



ע"י נק' פיתול על עקום אליפטי, כי נק' פיתול זו נק' מסדר 3.

איפה אפשר לקרוא עוד?

יש כל מיני ספרים, למשל של סילברמן (לא אלמנטרי), וושינגטון (יותר אלמנטרי), או ג'יימס מילן (ממש לא אלמנטרי).

תיהנו!