הרצאה: פולינומים ציקלוטומים ומשפט זיגמונדי, מחנה פסח 2015 / אופיר גורודצקי

(הערות/הארות/שאלות/תיקונים נא לשלוח ל־bambaman1@gmail.com)

1. בעיות

להלן רשימת 17 בעיות יפות שנוכל (לנסות ו)לפתור לאחר שנכיר את הנושא:

- משוואות דיופנטיות (נסו להכליל)

1. $p^x - y^q = \pm 1$ כאשר p, q ראשוניים
2. (Israel-Hungary 2006) $x^n + y^n = p^k$ כאשר p ראשוני ו־n אי־זוגי
3. (IMO Shortlist 2006) $y^5 - 1 = \frac{x^7-1}{x-1}$
4. $(ab+1)^m = 1 + a^n$

- גיאומטריה וטריגונומטריה

1. חשבו ומיצאו את $\prod_{k=1,(k,n)=1}^{n} \cos\frac{k\pi}{n}, \prod_{k=1,(k,n)=1}^{n} \sin\frac{k\pi}{n}$.[1]
2. יהי $\theta \in \mathbb{Q}$. הוכיחו כי:
   (א) $\sin\pi\theta \in \mathbb{Q} \implies \sin\pi\theta \in \{0, \pm 1, \pm\frac{1}{2}\}$
   (ב) $\cos\pi\theta \in \mathbb{Q} \implies \cos\pi\theta \in \{0, \pm 1, \pm\frac{1}{2}\}$
   (ג) $\tan\pi\theta \in \mathbb{Q} \implies \tan\pi\theta \in \{0, \pm 1\}$
3. הראו כי עבור $n > 2$, הפולינום המינימלי של $\cos(\frac{2\pi}{n})$ הוא ממעלה $\frac{\phi(n)}{2}$. ⋆ מצאו לו נוסחת רקורסיה בסגנון הכלה־הדחה.
4. יהיו $P_0, \cdots, P_{n-1}$ קודקודיו של מצולע משוכלל בין n קודקודים. תת־קבוצה של קודקודיו תיקרא "יציבה" אם מרכז המסה של איבריה מתלבד עם מרכז המסה של המצולע. מצאו תת־קבוצות אלו במקרה ש־n ראשוני ובמקרה ש־n חזקת ראשוני. ⋆ נסו גם את המקרה של מכפלת 2 ראשוניים שונים ומכפלת 2 חזקות ראשוניים.

- ראשוניים

1. הוכיחו כי אם $4^n + 2^n + 1$ ראשוני אזי $n = 3^k$.
2. הראו כי יש אינסוף ראשוניים מהצורה $1 \mod n$. ⋆ כמו כן, יש אינסוף ראשוניים מהצורה $-1 \mod n$.[2]
3. (IMO Shortlist 2002) יהיו $\{p_i\}_{i=1}^{n}$ ראשוניים אי־זוגיים שונים גדולים מ־3. הוכיחו כי ל־$2^{\prod_{i=1}^{n} p_i} + 1$ יש לפחות 2^{2^n} מחלקים.
4. הראו כי $p \equiv 1 \mod 4$ ראשוני גורר $\frac{p^p-1}{p-1}$ אינו ראשוני, בעוד $p \equiv 3 \mod 4 \wedge p \neq 3$ ראשוני גורר $\frac{p^p+1}{p+1}$ אינו ראשוני.

[1] רמז: הביעו את $\sin\frac{k\pi}{n}, \cos\frac{k\pi}{n}$ בעזרת $1 \pm \omega_n^k$ והשתמשו בערכי $\phi_n(\pm 1)$.

[2] רמז: עבור $n > 2$ נסמן ב־$\psi_n(x)$ את הפולינום (במקדמים שלמים!) המקיים $\phi_n(x)x^{-\frac{\phi(n)}{2}} = \psi_n(x + x^{-1})$. הראו שעבור x שלם, גורמיו הראשוניים הם $\pm 1 \mod n$ או מחלקים של $2n$. בצעו שינוי משתנים כך של־$a \cdot \psi_n(bx + c)$ יהיה מקדם חופשי -1.

5. (USAMO 2007) הראו ש־$7^{7^n}+1$ מכפלה של לפחות $2n+3$ גורמים ראשוניים (לאו דווקא שונים).

- <u>שונות</u>

1. יהיו $f,g:\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}$. אם הקונבולציה $(f*g)(k):=\sum_{i+j=k}f(i)g(j)$ מתאפסת (לכל k), הוכיחו כי גם הקונבולוציה של f עם $g(cx)$ מתאפסת בהנחה $(c,n)=1$.
2. (IMC 2010) ⋆ נניח כי $f:\mathbb{R}\to\mathbb{R}$ מתאפסת זהותית על איזשהו קטע I. בנוסף, לכל ראשוני p מתקיים $\sum_{k=0}^{p-1}f(x+\frac{k}{p})\equiv 0$. הסיקו ש־$f\equiv 0$.
3. הראו שמספרי פיבונאצ'י היחידים שהם גם מספרי קטלן הם $1,2,5$.
4. משפט וודרבורן (Wedderburn): אם R תחום (חוג ללא מחלקי אפס) סופי עם יחידה, אז הוא שדה.[3]

2. <u>פולינומים ציקלוטומים - הגדרות</u>

למה א': $\gcd(x^n-1,x^m-1)=x^{\gcd(n,m)}-1$. למה ב': ל־$x^n-1$ שורשים פשוטים ("פולינום ספרבילי").

כעת ניתן להגדיר:

1. $\phi_n(x)$ הוא הגורם שמופיע בפירוק של x^n-1 ולא בפירוק של הקודמים $\{x^d-1\}_{d<n}$.
2. הגדרה חמדנית:

$$\phi_n(x)=\frac{x^n-1}{\mathrm{GCD}(x^n-1,\prod_{d<n}(x^d-1))}=\frac{x^n-1}{\mathrm{LCM}_{d|n,d\neq n}(x^d-1)}=\frac{x^n-1}{\mathrm{LCM}_{p|n}(x^{n/p}-1)}=\mathrm{GCD}_{d|n,d\neq n}\frac{x^n-1}{x^d-1}=\mathrm{GCD}_{p|n}\frac{x^n-1}{x^{n/p}-1}$$

3. הגדרה רקורסיבית: $\prod_{d|n}\phi_d(x)=x^n-1$, ממנה (בעזרת היפוך מביוס, קרי: הכלה־הדחה): $\phi_n(x)=\prod_{d|n}(x^{n/d}-1)^{\mu(d)}$ כאשר $\mu(n)$ היא "פונקציית מביוס" - אם n הוא מכפלת k ראשוניים שונים אז $\mu(n)=(-1)^k$, ובכל מקרה בו n מתחלק פעמיים בראשוני, הפונקציה מקבלת 0.
4. הגדרה מפורשת: נסמן $\omega_n:=e^{\frac{2\pi i}{n}}\in\mathbb{C}$ (שורש יחידה פרימיטיבי מסדר n). מתקיים: $\phi_n(x)=\prod_{i=1,(i,n)=1}^{n}(x-\omega_n^i)$.

ניתן להראות את הגרירות $1\leftarrow 2\leftarrow 3\leftarrow 4$. בהמשך נראה כי לא רק ש־$\phi_n(\omega_n)=0$, אלא ש־$\phi_n$ הפולינום המינימלי של ω_n מעל הרציונלים.

3. <u>תכונות כלליות וקומבינטוריות</u>

1. אלמנטרי/מיידי: הפולינומים מתוקנים, בעלי מקדמים שלמים (מהלמה של גאוס, בתור גורם מתוקן של x^n-1. לחילופין, ל־ϕ_n מקדמים רציונלים מהגדרה 3, והם גם שלמים אלגברים כי השורשים שלמים אלגברים, על כן הם שלמים), ממעלה $\phi(n)$, ספרבילים וזרים בזוגות.
2. ⋆ אם n מתחלק בבדיוק 2 ראשוניים אז המקדמים של ϕ_n הם רק $-1,0,+1$, אך זה לא נכון ל־n כללי והם יכולים לקבל כל ערך שלם (תרגיל!).

[3] רמז: הראו שמדובר בחוג עם חילוק ע"י כך שההעתקה $x\mapsto ax$ היא חח"ע לכל $a\neq 0$. נשים לב שהמרכז של החוג הוא שדה סופי, ונניח בשלילה שהוא לא כל החוג. כעת נכתוב את איברי החוג בתור אוסף זר של מחלקות צמידות, נספור ונקבל משוואה דיופנטית ללא פתרונות.

3. מתקיים: $\phi_{np^k}(x) = \phi_n(x^{p^k})$ אם $p \mid n$, ואחרת $\phi_{np^k}(x) = \frac{\phi_n(x^{p^k})}{\phi_n(x^{p^{k-1}})}$. באופן כללי יותר, $\phi_n(x^m) = \prod_{d|m,(d,n)=1} \phi_{\frac{nm}{d}}(x)$
$\phi_{\prod p_i^{a_i}}(x) = \phi_{\prod p_i}(x^{\prod p_i^{a_i-1}})$ ו־.

4. אם $n > 1$ אז הפולינומים הם סימטריים (בפרט: מקדם חופשי 1), המקדם של x הוא $-\mu(n)$, וסכום המקדמים $\phi_n(1)$ יוצא $\prod_{d|n} d^{\mu(n/d)} = \begin{cases} 1 & n \neq p^k \\ p & n = p^k \end{cases}$. (נסו לחשב את המקדם של x^2 ואת $\phi_n(-1)$.)

4. תכונות אריתמטיות

- **גורמים** (הטענה החשובה של ההרצאה!)

עבור מספר טבעי x, אם p מחלק את $\phi_n(x)$, מתקיים אחד מהשניים: $p \equiv 1 \mod n$, או ש־p מחלק את n.

למעשה, p מהסוג הראשון מקיים: $\mathrm{ord}_p(x) = n$ ולכן $p \nmid \prod_{d<n} \phi_d(x)$, ו־$p$ מהסוג השני הוא בהכרח הראשוני המקסימלי המחלק את n, וריבויו לכל היותר 1 (מלבד אולי המקרה $n = 2$).

הוכחה: יהי p גורם ראשוני של $\phi_n(x)$. בפרט, $x^n \equiv 1 \mod p$ ולכן $\mathrm{ord}_p(x) \mid n$. אם יש שיוויון $\mathrm{ord}_p(x) = n$), אז בגלל המשפט הקטן של פרמה ($\mathrm{ord}_p(x) \mid p-1$) נובע $p \equiv 1 \mod n$.

אם אין שיוויון, נובע שלפולינום $t^n - 1$ יש גורם כפול מודולו p (מתחלק ב־$\phi_{\mathrm{ord}_p(x)}(t), \phi_n(t)$ ששניהם מתאפסים ב־x). לכן יש לו gcd לא טריוויאלי עם נגזרתו, $nt^{n-1} \mod p$. בגלל שאפס אינו שורש שלו, בהכרח $n \equiv 0 \mod p$, או: $p \mid n$.

ניתן להגיד יותר מכך. נסמן ב־q גורם ראשוני של $\frac{n}{\mathrm{ord}_p(x)}$. מההגדרה מתקיים: $x^{\frac{n}{q}} \equiv 1 \mod p$. אבל $p \mid \phi_n(x) \mid \frac{x^n-1}{x^{\frac{n}{q}}-1} = \sum_{i=0}^{q-1} x^{\frac{n}{q}i} \equiv \sum_{i=0}^{q-1} 1^i \mod p$, לכן: $0 \equiv q \mod p$, כלומר $p \mid q$. מהראשוניות, $p = q$. אבל q גורם ראשוני שרירותי של $\frac{n}{\mathrm{ord}_p(x)}$, לכן $\frac{n}{\mathrm{ord}_p(x)} = p^{\alpha \geq 1}$. בגלל ש־$\mathrm{ord}_p(x) \leq p-1$, אנחנו מקבלים ש־$p$ הגורם הראשוני המקסימלי המחלק את n. אם נעבוד מודלו p^2 נוכל לחשב ריבוי: $\phi_n(x) \mid \frac{x^n-1}{x^{\frac{n}{p}}-1}$, ואם נכתוב $x^{\frac{n}{p}} = 1 + tp$ נקבל $\frac{x^n-1}{x^{\frac{n}{p}}-1} = \frac{(1+tp)^p-1}{tp} \equiv p + tp\binom{p}{2} \mod p^2$. אם $p > 2$ אז ביטוי זה שווה $p \mod p^2$ ולכן הריבוי של p הוא 1. אם $p = 2$ אז $n = 2^k$ ולכן $\phi_n(x) = x^{2^{k-1}} + 1$. בגלל שריבוע שווה 0 או 1 מודולו 4, כדי שביטוי זה יתחלק פעמיים ב־4 נדרש $k = 1$, כלומר: $n = 2$. ■

- **גורמים כפולים**

אם ל־$\phi_n(x)$ גורם כפול ב־$\mathbb{F}_p[x]$ אז $p \mid n$. הוכחה: נראה שכאשר $p \nmid n$, אין גורם כפול, כלומר: $\gcd(\phi_n(x), \phi_n'(x)) \neq 1$ כשעובדים ב־$\mathbb{F}_p[x]$. אם נגזור את $x^n - 1$ (כפולה של $\phi_n(x)$) נקבל קומבינציה לינארית של $\phi_n(x), \phi_n'(x)$ ששווה nx^{n-1}, שזר ל־$\phi_n(x)$ מודולו p. ■

הכיוון השני כמעט נכון: אם $p \mid n$, אז מתקיים $\phi_n(x) = \phi_{\frac{n}{p}}(x^p) \equiv \phi_{\frac{n}{p}}^p(x) \mod p$ או $\phi_n(x) = \frac{\phi_{\frac{n}{p}}(x^p)}{\phi_{\frac{n}{p}}(x)} \equiv \phi_{\frac{n}{p}}^{p-1}(x) \mod p$. כאשר $p > 2$ יש אוטומטית גורם כפול, וכאשר $p = 2$ נדרש $4 \mid n$.

⋆ למעשה, הדיסקרימיננטה של ϕ_n, המוגדרת בתור $\prod_{i>j,(i,n)=(j,n)=1}(\omega_n^i - \omega_n^j)^2$, שווה $(-1)^{\phi(n)/2} \frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}$.

(תזכורת: לפולינום יש גורם כפול מודולו p אמ"מ הדיסקרימיננטה שלו מתחלקת ב־p.)

- **אי־פריקות**

הם אי־פריקים. עבור $n = p^k$ זה נובע מקריטריון איזנשטיין עבור $\phi_n(x+1)$.

<u>הוכחה עבור n כללי:</u>

דרך א': מספיק להראות שפולינום אי־פריק $g(x)$ שמתאפס ב־ω_n חייב להתאפס גם ב־ω_n^i לכל $(i,n) = 1$. בשביל זה מספיק להראות שאם הפולינום מתאפס ב־z אז הוא מתאפס ב־z^p, לכל ראשוני $p \nmid n$. נשים לב ש־$g(x) \mid \phi_n(x)$ נניח בשלילה ש־$g(z) = 0, g(z^p) \neq 0$. נכתוב: $\phi_n(x) = g(x)h(x)$. ϕ_n מתאפס ב־z^p ולכן בהכרח h גם מתאפס ב־z^p. אם נעבוד ב־$\mathbb{F}_p \cong \mathbb{Z}[z]/(1-z)$ נקבל: $\overline{h}(\overline{z})^p = \overline{h}(\overline{z^p}) = \overline{0}$, כלומר $\overline{h}(\overline{z}) = \overline{g}(\overline{z}) = 0$ ול־$\phi_n(x)$ שורש כפול מודולו p מה שגורר $p \mid n$, סתירה. ■

<u>הערה:</u> היינו רוצים לנסח את סוף ההוכחה ללא שימוש בתורת מספרים אלגברית ובפרט ללא $\mathbb{Z}[z]/(1-z) \cong \mathbb{F}_p$. זה אפשרי כך: $h(x^p)$ מתאפס ב־z כי $h(x)$ מתאפס ב־z^p. לכן $g(x) \mid h(x^p)$. מודולו p נקבל ש־$\overline{h(x)}^p = \overline{h(x^p)} \mid \overline{g(x)}$, ולכן $\overline{h(x)} \mid \overline{g(x)}$. מכאן ש־$\overline{\phi_n}$ מתחלק פעמיים ב־$\overline{g}$, בסתירה לכך שאין ל־ϕ_n גורמים כפולים מודולו p כאשר $p \nmid n$. ■

דרך ב': ⋆ נשים לב שמספיק להראות שמעלת הרחבת גלואה $\mathbb{Q}(\omega_n)/\mathbb{Q}$ היא $\phi(n)$. צפיפות הראשוניים הרציונליים המתפצלים היא $\frac{1}{[\mathbb{Q}(\omega_n):\mathbb{Q}]}$ מצד אחד (משפט הצפיפות של צ'בוטרב), ומצד שני זה שקול להתפצלות (=התפרקות לגורמים לינאריים זרים) של הפולינום $x^n - 1 \mod p$, ששקולה ל־$p \equiv 1 \mod n$, וממשפט דיריכלה הצפיפות של ראשוניים אלו היא $\frac{1}{\phi(n)}$. ■

- **גורמים משותפים**

יהי x שלם. בעקבות הבנתנו את הגורמים של $\phi_n(x)$, קל לראות כי אם p מחלק את $\phi_n(x), \phi_m(x)$ כאשר $n > m$ אז $m|n$ ו־$\frac{n}{m}$ שווה חזקה של p. p חייב להיות הגורם המקסימלי של n ולהופיע בריבוי 1 ב־$\phi_n(x)$. בפרט, $\gcd(\phi_n(x), \phi_m(x))$ שווה 1 או ראשוני p (כאשר בהכרח p הראשוני המקסימלי המחלק את n ו־$\frac{n}{m}$ חזקת p).

⋆ למעשה, הרזולטנטה של $\phi_n(x), \phi_m(x)$, המוגדרת בתור $\prod_{(i,n)=(j,m)=1}(\omega_n^i - \omega_m^j)$, שווה
$$\begin{cases} 1 & \frac{n}{m} \neq p^k \\ p^{\phi(m)} & \frac{n}{m} = p^k \end{cases}.$$

(תזכורת: לזוג פולינומים יש גורם משותף מודולו p אמ"מ הרזולטנטה שלהם מתחלקת ב־p.)

ניתן להראות באמצעות בנייה מפורשת שהאידאל $(\phi_n(x), \phi_m(x)) \cap \mathbb{Z}$ נוצר ע"י p אם $\frac{n}{m} = p^k$, ואחרת ע"י 1. (באופן כללי, היוצר של $(f(x), g(x)) \cap \mathbb{Z}$ מחלק את $\mathrm{Res}(f,g)$ אך לאו דווקא שווה לו).

- **שדות סופיים**

ב־$\mathbb{F}_q[x]$, בהנחת $(n,q) = 1$, $\phi_n(x)$ מתפרק ל־$\frac{\phi(n)}{\mathrm{ord}_n(q)}$ אי־פריקים ממעלה $\mathrm{ord}_n(q)$. בפרט, $\phi_8(x) = x^4 + 1$ פולינום אי־פריק בשלמים שמתפרק מודולו כל ראשוני.

- **נוסחאות גאוס־לוקאס**

לכל n אי־זוגי נטול ריבועים גדול מ־3,

$$\exists R, S \in \mathbb{Z}[x] : 4 \cdot \phi_n(x) = R(x)^2 - (-1)^{\frac{n-1}{2}} n S(x)^2$$

$$\exists R, S \in \mathbb{Z}[x] : \phi_n(x) = R(x)^2 - (-1)^{\frac{n-1}{2}} n x S(x)^2$$

הוכחה: ⋆ נוכיח את הנוסחה הראשונה ומתוכה נסיק את השנייה. חבורת גלואה של $\mathbb{Q}(\omega_n)$ מעל $\mathbb{Q}$ איזומורפית ל־$(\mathbb{Z}/n\mathbb{Z})^\times$). יש לה תת־חבורה (נורמלית) מאינדקס 2: $G_n := \{a \in (\mathbb{Z}/n\mathbb{Z})^\times | (\frac{a}{n}) = 1\}$. שדה השבת של תת־חבורה זו נותן הרחבה ריבועית של $\mathbb{Q}$: $\mathbb{Q}(\sqrt{D})$. סכום גאוס $\sum_{a=0}^{n-1}(\frac{a}{n})\omega_n^a \in \mathbb{Q}(\omega_n)$ נמצא בשדה שבת זה וריבועו שווה $n^* := n(-1)^{\frac{n-1}{2}}$, על כן $D = n^*$. המקדמים של הפולינום $\psi_n(x) := \prod_{1\le i\le n,(\frac{i}{n})=1}(x-\omega_n^i)$ נמצאים בשדה השבת גם כן, והם שלמים אלגברים, לכן מקדמיו נמצאים בחוג השלמים של $\mathbb{Q}(\sqrt{n^*})$, שהוא $\mathbb{Z}[\frac{1+\sqrt{n^*}}{2}]$, לכן אפשר לכתוב $\psi_n(x) = \frac{R(x)+\sqrt{n^*}S(x)}{2}$. נכפול כל אחד מהאגפים בצמוד גלואה שלו ונקבל $\phi_n(x) = \frac{R(x)^2-n^*S(x)^2}{4}$.

את הנוסחה השנייה מסיקים מהראשונה ע"י כך שנכתוב $\phi_n(x^2) = \phi_n(x)\phi_n(-x)$ ונשתמש בנוסחה הראשונה (צריך להוכיח כמה עובדות על R, S, ביניהן: $S(0) = 0$). ■

5. משפט זיגמונדי (Zsigmondy)

- נניח $a > b > 0$ זרים. ל־$a_n = a^n - b^n$ קיים מחלק ראשוני פרימיטיבי, קרי: שלא מחלק את $\{a^i - b^i\}_{i<n}$, מלבד במקרים $(a, b, n) \in \{(b+1, b, 1), (2, 1, 6), (a, 2^k - a, 2)\}$.
- מסקנה: הטענה נכונה גם ל־$\frac{a_{2n}}{a_n} = a^n + b^n$. יוצאי הדופן: $(a, b, n) \in \{(2, 1, 3), (1, 2, 3)\}$.

הוכחה:

(נתרכז במקרה $a_n = x^n - 1$ עם $x > 1$ ־ המקרה הכללי ישאר כתרגיל שמוכח בדיוק באותו אופן.)

ברור ש־$a_n \mid \phi_n(x)$. מהיכרותנו עם הגורמים של $\phi_n(x)$, יש 3 מקרים:

- אם $n = 1$, $\phi_n(x) = x - 1$ והטענה טריוויאלית אלא אם $x - 1 = 1$, כלומר אם $x = 2$.
- אם $n = 2$, $\phi_n(x) = x + 1$. גורם ראשוני שלו שאינו פרימיטיבי יכול להיות רק $p = 2$. זה גורר ש־$x + 1 = 2^{k\ge 1}$.
- $n > 2$. נניח בשלילה שאין גורמים פרימיטיבים, קרי: $\phi_n(x) = \pm q$ כאשר q הגורם הראשוני המקסימלי המחלק את n.

נתמודד עם המקרה השלישי. אם $q = 2$ אז $n = 2^s$ ולכן $2 = q = |\phi_n(x)| = x^{2^{s-1}} + 1$, כלומר $x = 1$, סתירה.

אם $q > 2$, נכתוב $n = q^i r$ ונקבל:

$$q = |\phi_n(x)| = |\frac{\phi_r(x^{q^i})}{\phi_r(x^{q^{i-1}})}| = \prod_{(j,\phi(r))=1} |\frac{x^{q^i}-\omega_r^j}{x^{q^{i-1}}-\omega_r^j}| > (\frac{x^{q^i}-1}{x^{q^{i-1}}+1})^{\phi(r)} \ge \frac{x^{q^i}-1}{x^{q^{i-1}}+1} \ge x^{q^{i-1}(q-2)} \ge 2^{q-2}$$

מה שגורר $q = 3$. כשנציב בשרשרת האי־שיוויונים נקבל $x = 2, i = 1$. נסיק ש־$n \in \{3, 6\}$, כי $r = 1$ או $r = 2$.

אם $n = 3$: $\phi_n(x) = 7$ ־ 7 גורם פרימיטיבי (סתירה). לכן $n = 6$: $\phi_n(x) = 3$ ־ וזה אכן מקרה יוצא דופן כי $3 \mid \phi_2(x)$. ■

6. משפט קרמייקל (Carmichael)

- נגדיר $D_n := \frac{\alpha^n-\beta^n}{\alpha-\beta}$ כאשר α, β שורשים של משוואה ריבועית $x^2 + ax + b = 0$ ("סדרת לוקאס"), תחת התנאים ש־a, b שלמים זרים ו־$a^2 - 4b$ חיובי.

- בתנאים אלה ל־D_n קיים מחלק ראשוני פרימיטיבי, קרי: שלא מחלק את $\{D_i\}_{1\leq i<n}$, מלבד במקרים $n\in\{1,2,6\}$ ו־$(n,a,b)=(12,-1,-1)$.
- מסקנה: נכון גם ל־$\tilde{D}_n=\frac{D_{2n}}{D_n}=\alpha^n+\beta^n$, עם יוצאי הדופן $n\in\{1,3,6\}$.
- מסקנה נוספת: המשפט נכון עבור סדרת פיבונאצ'י F_n ($F_0=0,F_1=1,F_{n+2}=F_{n+1}+F_n$), מלבד יוצאי הדופן $n\in\{1,2,6,12\}$.

<u>הוכחה:</u>

נגדיר $\phi_n(\alpha,\beta):=\phi_n(\frac{\beta}{\alpha})\alpha^{\phi(n)}$ עבור $n>1$, ו־$\phi_1(\alpha,\beta):=1$. אלו מספרים שלמים ומתקיים: $D_n=\prod_{d|n}\phi_d(\alpha,\beta)$. על כן, p גורם פרימיטיבי של D_n אמ"מ הוא גורם פרימיטיבי של $\phi_n(\alpha,\beta)$. כעת נזדקק למספר למות:

1. אם $n\notin\{1,2,6\}$ ו־p גורם לא פרימיטיבי של D_n, אז ריבויו ב־D_n הוא 1. בנוסף, n הוא מהצורה p^rk, כאשר k הוא המספר הקטן ביותר כך ש־$p\mid D_k$.
2. מסקנה מהלמה הקודמת: בהנחה ש־$n\notin\{1,2,6\}$, תנאי מספיק לכך של־D_n יש גורם פרימיטיבי הוא $|\phi_n(\alpha,\beta)|>\prod_{p|n}p$.
3. יהיו (α_1,β_1) שורשי $x^2-x-1=0$, ו־(α_2,β_2) שורשי $x^2-3x+2=0$. אם האי־שיוויון מלמה 2 מתקיים עבור 2 זוגות אלו, אז הוא מתקיים בכל המקרים הרלוונטים למשפט.
4. אם $n>2$ ו־t מספר ממשי המקיים $|t|<\frac{1}{2}$, אז $\phi_n(t)\geq 1-|t|-|t|^2$.

רק הלמה הראשונה היא תורת המספרים. בהינתן הלמות, ההוכחה הולכת כך:

עבור המקרה של פיבונאצ'י ($x^2-x-1=0$) נפעל כך: נניח $n\notin\{1,2,6\}$. מתקיים $\phi_n(\alpha,\beta)>\frac{2}{5}(\frac{3}{2})^{\phi(n)}$ לפי למה 4, ואנחנו רוצים: $\frac{2}{5}(\frac{3}{2})^{\phi(n)}\geq\prod_{p|n}p$. עבור $n>30$ אפשר לוודא שאי־שיוויון זה מתקיים משיקולים פשוטים יחסית, ובעזרת חישובים ישירים עבור הערכים הקטנים נקבל שאי־השיוויון של למה 2 נכון למעשה לכל $n\neq 1,2,3,5,6,12$. במקרים שנותרו נבדוק את F_n ונראה שיש לו גורם פרימיטיבי או ש־n כלול בין יוצאי הדופן.

עבור המקרה $x^2-3x+2=0$ נפעל בדומה: נניח $n\notin\{1,2,6\}$. מתקיים $\phi_n(\alpha,\beta)>\frac{1}{4}2^{\phi(n)}$ לפי למה 4, ואנחנו רוצים: $\frac{1}{4}2^{\phi(n)}\geq\prod_{p|n}p$. הוא נכון עבור $n\neq 1,2,3,4,5,6,10,12$. במקרים $n=3,4,5,6,10,12$ בודקים ידנית ומתקיים $|\phi_n(\alpha,\beta)|>\prod_{p|n}p$.

מלמה 3, כדי לפתור את המקרה הכללי מספיק לבדוק את $n=1,2,3,5,6,12$. נשאיר זאת לקורא. ■

<u>הערה:</u> משפטים דומים הוכחו גם למקרה ש־a^2-4b שלילי, כלומר α,β מרוכבים.

לקריאה נוספת בנושא פולינומים ציקלוטומים, ראו פוסט "פולינומים ציקלוטומים ומשפט זיגמונדי" בבלוג oneand.wordpress.com.