חשבון מודולרי - הוכחות נבחרות

תורת המספרים האלמנטרית - 80115

מרצה: אהוד (אודי) דה-שליט

מתרגל: גיא ספיר

סוכם ע"י: שריה אנסבכר

סמסטר ב' תשפ"ג, האונ' העברית

תוכן העניינים

תודתי נתונה לאורטל פלדמן על הסיכום שכתב בשנת הלימודים תשע"ו,
נעזרתי בו רבות על מנת לכתוב את הסיכום שלפניכם.

* * *

אשמח לקבל הערות והארות על הסיכומים על מנת לשפרם בעתיד,
כל הערה ולו הפעוטה ביותר (אפילו פסיק שאינו במקום או רווח מיותר) תתקבל בברכה;
אתם מוזמנים לכתוב לי לתיבת הדוא"ל: sraya.ansbacher@mail.huji.ac.il.

לסיכומים נוספים היכנסו לאתר:
אקסיומת השלמות - סיכומי הרצאות במתמטיקה
https://srayaa.wixsite.com/math

1 התחלה

♣ אודי קרא לנושא הזה לזה גם "חשבון בקונגרואנציות"...

יהי $1 < N \in \mathbb{N}$.

1.1 משפטים בסיסיים

למה 1.1. יהי $f \in \mathbb{Z}[x]$, לכל $x, y \in \mathbb{Z}$ המקיימים $x \equiv y \mod N$ מתקיים $f(x) \equiv f(y) \mod N$.

טענה 1.2. יהי $f \in \mathbb{Z}[x]$ אם קיים $x \in \mathbb{Z}$ כך ש-$f(x) = 0$ אז אותו x מקיים $\overline{f(x)} = \overline{0}$.

♣ השימוש המרכזי של טענה זו הוא הוכחה שלפולינום נתון אין שורשים בכך שנראה שאין לו שורשים מודולו N (כאשר את N נוכל לבחור בעצמנו).

♣ למעשה ניתן להרחיב את הטענה: לכל משוואה שיש לה פתרון בשלמים יש לה גם פתרון בכל חוג שלמים מודולו N, לכן אם ברצוננו להראות שלמשוואה מסוימת בשלמים אין פתרון נוכל לבחור מודולוס כאוות נפשנו (כמובן שיש לבחור אותו בצורה אסטרטגית וזה החלק הכי מסובך בעניין) ולהראות שבחוג המודולרי שלו אין פתרון למשוואה.

טענה 1.3. לכל $x, y \in \mathbb{Z}$ ולכל $n \in \mathbb{Z}$, אם $x \equiv y \mod N$ וגם $n \mid N$ אז $x \equiv y \mod n$.

טענה 1.4. לכל $x, y \in \mathbb{Z}$ ולכל $0 \neq a \in \mathbb{Z}$ מתקיים:

$$ax \equiv ay \mod N \iff x \equiv y \mod \frac{N}{\gcd(a, N)}$$

מסקנה 1.5. כלל הצמצום

לכל $x, y \in \mathbb{Z}$ ולכל $0 \neq a \in \mathbb{Z}$ הזר ל-N מתקיים:

$$ax \equiv ay \mod N \iff x \equiv y \mod N$$

משפט 1.6. למשוואה מהצורה $ax \equiv b \mod N$ יש פתרון אם"ם $\gcd(a, N) \mid b$, במקרה כזה ניתן להמיר אותה (ע"פ טענה 1.4) למשוואה (נגדיר $d := \gcd(a, N)$):

$$\frac{a}{d} \cdot x \equiv \frac{b}{d} \mod \frac{N}{d}$$

ואז $\frac{a}{d}$ זר ל-$\frac{N}{d}$ ולכן יש לו הופכי מודולרי והפתרונות מוכרחים לקיים:

$$x \equiv \left(\frac{a}{d}\right)^{-1} \cdot \frac{b}{d} \mod \frac{N}{d}$$

♣ נשים לב לכך שקיום פתרון יחיד מודולו $\frac{N}{d}$ אומר שישנם d פתרונות מודולו N.

♣ ניתן למצוא ההופכי המודולרי ע"י אלגוריתם אוקלידס המורחב: יהיו $s, t \in \mathbb{Z}$ מספרים זרים, האלגוריתם נותן לנו $n, m \in \mathbb{Z}$ כך ש-$1 = n \cdot s + m \cdot t$ ומכאן ש-$n \cdot s \equiv 1 \mod t$ ו-$m \cdot t \equiv 1 \mod s$, כלומר n הוא ההופכי של s מודולו t ו-m הוא ההופכי של t מודולו s (היחידות היא עד כדי שקילות מודולרית כמובן).

טענה 1.7. הקבוצה $(\mathbb{Z}/N\mathbb{Z})^*$ סגורה תחת כפל, כלומר לכל $\overline{a}, \overline{b} \in (\mathbb{Z}/N\mathbb{Z})^*$ מתקיים $\overline{a} \cdot \overline{b} \in (\mathbb{Z}/N\mathbb{Z})^*$.

1.2 המשפט הקטן של פרמה, פונקציית אוילר ומשפט השאריות הסיני

משפט 1.8. המשפט הקטן של פרמה
יהי $p \in \mathbb{N}$ מספר ראשוני, לכל $a \in \mathbb{Z}$ כך ש-$a \not\equiv 0 \mod p$ מתקיים $a^{p-1} \equiv 1 \mod p$.

הוכחה. נוכיח את המשפט הקטן של פרמה שנוכיח את משפט אוילר (משפט 1.12). ■

מסקנה 1.9. יהי $p \in \mathbb{N}$ ראשוני, לכל $a \in \mathbb{Z}$ כך ש-$a \not\equiv 0 \mod p$ ולכל $i, j \in \mathbb{N}$, מתקיים $a^i \equiv a^j \mod N$ אם"ם $i \equiv j \mod p-1$.

♣ המסקנה מראה לנו שמהמשפט הקטן של פרמה נובע שכדי לחשב חזקות בחשבון מודולו p ניתן לבצע חשבון מודולו $p-1$ על המעריך.

מסקנה 1.10. יהי $p \in \mathbb{N}$ מספר ראשוני, לכל $a \in \mathbb{Z}$ מתקיים $a^p \equiv a \mod p$.

למה 1.11. יהי $a \in \mathbb{Z}$ זר ל-N ויהיו $r_1, r_2, \ldots, r_{\phi(N)} \in \mathbb{Z}$ כך ש-$\left\{\overline{r_1}, \overline{r_2}, \ldots, \overline{r_{\phi(N)}}\right\} = (\mathbb{Z}/N\mathbb{Z})^*$, מתקיים $\left\{\overline{a \cdot r_1}, \overline{a \cdot r_2}, \ldots, \overline{a \cdot r_{\phi(N)}}\right\} = (\mathbb{Z}/N\mathbb{Z})^*$.

משפט 1.12. משפט אוילר
לכל $a \in \mathbb{Z}$ כך ש-a זר ל-N מתקיים $a^{\phi(N)} \equiv 1 \mod N$.

הוכחה. נשתמש בסימונים של הלמה האחרונה ונשים לב לכך שנובע ממנה כי:

$$a^{\phi(N)} \cdot \prod_{i=1}^{\phi(N)} r_i = \prod_{i=1}^{\phi(N)} (a \cdot r_i) \equiv \prod_{i=1}^{\phi(N)} r_i \mod N$$

כעת נזכר שכל האיברים במכפלה שבאגף ימין הפיכים ולכן גם המכפלה עצמה הפיכה וניתן לצמצם בה את שני האגפים, כלומר $a^{\phi(N)} \equiv 1 \mod N$ כנדרש. ■

♣ משפט אוילר הוא הכללה של המשפט הקטן של פרמה.

מסקנה 1.13. לכל $a \in \mathbb{Z}$ זר ל-N ולכל $i, j \in \mathbb{N}$, מתקיים $a^i \equiv a^j \mod N$ אם"ם $i \equiv j \mod \phi(N)$.

♣ המסקנה מראה לנו שממשפט אוילר נובע שכדי לחשב חזקות בחשבון מודולו N ניתן לבצע חשבון מודולו $\phi(N)$ על המעריך וזאת בתנאי שהבסיס זר ל-N.

משפט 1.14. משפט השאריות הסיני (CRT - Chinese Remainder Theorem)
יהיו $1 < m_1, m_2, \ldots, m_k \in \mathbb{N}$ זרים זה לזה בזוגות ונסמן $m := \prod_{i=1}^{k} m_i$, לכל $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ קיים $m > x \in \mathbb{N}_0$ יחיד המקיים[1]:

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_k \mod m_k \end{aligned}$$

♣ ממשפט השאריות הסיני נובע שכדי שנוכל לפתור קונגרואנציה כלשהי ב-$\mathbb{Z}/N\mathbb{Z}$ די שנדע לפתור אותה מודולו $p^{\mathrm{Ord}_p(N)}$ לכל p ראשוני המחלק את N.

[1] כלומר קיים פתרון יחיד מודולו m, או אם תרצו: כל שני פתרונות שקולים מודולו m.

♣ כדי לקבל אינטואיציה למשפט השאריות הסיני נדמיין שני גלגלי שיניים המשתלבים זה בזה כך שמספר השיניים בגלגל אחד זר למספר השיניים בגלגל האחר, ברור לנו מבחינה אינטואיטיבית שבגלל שאין להם מחלק משותף (1 לא נחשב) נוכל להגיע להשתלבות של כל שן בגלגל האחד עם כל שן בגלגל האחר[2]; עבור מספר גדול יותר של גלגלי שיניים נשתמש באינדוקציה. כמובן שאפשר ממש לפרמל את האינטואיציה הזו לכדי הוכחה מתמטית, ראו את ההוכחה השלישית של המשפט.

נביא שלוש הוכחות שהן בעצם שתיים.

הוכחה. הוכחה 1 - לא קונסטרוקטיבית

יהיו $1 < m_1, m_2, \ldots, m_k \in \mathbb{N}$ זרים זה לזה בזוגות ונסמן $m := \prod_{i=1}^{k} m_i$.

תהא $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \ldots \times \mathbb{Z}/m_k\mathbb{Z}$ המוגדרת ע"י (לכל $[x]_m \in \mathbb{Z}/m\mathbb{Z}$):

$$f\left([x]_m\right) := \left([x]_{m_1}, [x]_{m_2}, \ldots, [x]_{m_k}\right)$$

מטענה 1.3 נובע ש-f אינה תלויה בבחירת הנציג ולכן מוגדרת היטב.

נוכיח ש-f חח"ע ומכאן שהיא גם על שהרי התחום והטווח שלה הן קבוצות סופיות שגודלן זהה.

יהיו $x, y \in \mathbb{Z}$ כך ש-$x \equiv y \mod m_i$ לכל $k \geq i \in \mathbb{N}$, א"כ מתקיים $m_i \mid x-y$ לכל $k \geq i \in \mathbb{N}$ ומכאן שגם $\operatorname{lcm}\left(m_1, m_2, \ldots, m_k\right) \mid x - y$.

כעת נשים לב לכך שמכיוון ש-$m_1, m_2, \ldots, m_k$ זרים זה לזה מתקיים בהכרח:

$$\operatorname{lcm}\left(m_1, m_2, \ldots, m_r\right) = \prod_{i=1}^{k} m_i = m$$

ומכאן ש-$x \equiv y \mod m$ ומהגדרה f חח"ע.

התחום והטווח של f הן קבוצות סופיות בגודל זהה ולכן עובדת היותה של f חח"ע אומרת ש-f גם על ולכן הפיכה, כלומר לכל $(a_1, a_2, \ldots, a_k) \in \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \ldots \times \mathbb{Z}/m_k\mathbb{Z}$ קיימת $x \in \mathbb{Z}/m\mathbb{Z}$ יחידה כך שמתקיים:

$$f(x) = (a_1, a_2, \ldots, a_k)$$

ומכאן שלכל $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ קיים $m > x \in \mathbb{N}_0$ יחיד כך שמתקיים:

$$\begin{aligned}
x &\equiv a_1 \mod m_1 \\
x &\equiv a_2 \mod m_2 \\
&\vdots \\
x &\equiv a_k \mod m_k
\end{aligned}$$

■

♣ ניתן היה גם להוכיח ש-f על ולכן מהשוויון בין הגדלים של התחום והטווח נובע שהיא חח"ע, ראו הדגמה לכך בהוכחה הראשונה של טענה 1.17.

[2] הפירמול של אינטואיציה זו הוא הידיעה שניתן להציג את 1 כצר"ל של שני המספרים ואם אנחנו מסוגלים לקבל את 1 מודולו n ע"י כפולות של m אנחנו יכולים לקבל כל שארית מודולרית מודולו n ע"י כפולות של m.

הוכחה. הוכחה 2 - קונסטרוקטיבית

יהיו $1 < m_1, m_2, \ldots, m_k \in \mathbb{N}$ זרים זה לזה בזוגות ונסמן $m := \prod_{i=1}^{k} m_i$.

לכל $k \geq i \in \mathbb{N}$ נסמן $n_i := \frac{m}{m_i}$, א"כ $\gcd(n_i, m_i) = 1$ לכל $k \geq i \in \mathbb{N}$ ולכן לכל $k \geq i \in \mathbb{N}$ קיימים $r_i, s_i \in \mathbb{Z}$ כך ש-$r_i \cdot m_i + s_i \cdot n_i = 1$.

א"כ יהיו r_i, s_i כנ"ל ונסמן $x_i := s_i \cdot n_i$ (כל זה לכל $k \geq i \in \mathbb{N}$ בנפרד), כעת נשים לב לכך שלכל $k \geq i, j \in \mathbb{N}$ מתקיים $x_i \equiv \delta_{ij} \mod m_j$[3] ולכן אם נסמן:

$$x := \sum_{i=1}^{k} a_i \cdot x_i$$

נקבל שמתקיים $x \equiv a_i \mod m_i$ לכל $k \geq i \in \mathbb{N}$.

כפי שראינו בהוכחה הקודמת לכל $y \in \mathbb{Z}$ כך ש-$x \equiv y \mod m$ מתקיים גם כן $y \equiv a_i \mod m_i$ ולכן בהכרח קיים $m > x \in \mathbb{N}_0$ המקיים זאת, היחידות נובעת מעקרון שובך היונים. ■

הוכחה. הוכחה 3 - הוכחה 2 רק באינדוקציה

נוכיח את המשפט באינדוקציה על k, עבור $k = 1$ המשפט טריוויאלי ולכן נעבור לצעד האינדוקציה.

יהי $k \in \mathbb{N}$, יהיו $1 < m_1, m_2, \ldots, m_k \in \mathbb{N}$ זרים זה לזה בזוגות ו-$a_1, a_2, \ldots, a_k \in \mathbb{Z}$; נניח שקיים $x \in \mathbb{Z}$ כך שמתקיים (הנחת האינדוקציה):

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_k \mod m_k \end{aligned}$$

ויהי x כנ"ל.

יהי $1 < m_{k+1} \in \mathbb{N}$ כך ש-$\gcd(m_{k+1}, m_i) = 1$ לכל $k \geq i \in \mathbb{N}$ ויהא $a_{k+1} \in \mathbb{Z}$.

נסמן $m := \prod_{i=1}^{k} m_i$, מהגדרה מתקיים $\gcd(m_{k+1}, m) = 1$ ולכן קיימים $r, s \in \mathbb{Z}$ כך ש-$r \cdot m_{k+1} + s \cdot m = 1$, יהיו r, s כנ"ל.

$$\begin{aligned} &\Rightarrow a_{k+1} - x = (a_{k+1} - x) \cdot r \cdot m_{k+1} + (a_{k+1} - x) \cdot s \cdot m \\ &\Rightarrow a_{k+1} - x \equiv (a_{k+1} - x) \cdot s \cdot m \mod m_{k+1} \\ &\Rightarrow a_{k+1} \equiv x + (a_{k+1} - x) \cdot s \cdot m \mod m_{k+1} \end{aligned}$$

כמובן שמתקיים $x + (a_{k+1} - x) \cdot s \cdot m \equiv x \mod m$ ולכן $x + (a_{k+1} - x) \cdot s \cdot m \equiv a_i \mod m_i$ לכל $k \geq i \in \mathbb{N}$.

א"כ הוכחנו את הקיום של הפתרון, היחידות נובעת כרגיל מעקרון שובך היונים. ■

[3] δ_{ij} (הדלתא של קרונקר) מוגדרת ע"י:

$$\delta_{ij} := \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

♣ אני רוצה להביא כאן המחשה קטנה לחשיבות האינטואיטיבית של העובדה שעבור מספרים זרים ניתן להציג את 1 כצר"ל שלהם:

$$\begin{aligned} x &\equiv 1 \mod 3 \\ x &\equiv 2 \mod 5 \\ x &\equiv 2 \mod 7 \end{aligned}$$

אמנם ניתן לפתור זאת ע"פ ההוכחה השנייה שלמדנו אולם ישנה דרך דומה אבל קצרה הרבה יותר כשמדובר במספרים קטנים:

$$\begin{aligned} & 3 \cdot 2 \equiv 6 \equiv 1 \mod 5 \\ & 2 - 1 = 1 \equiv 1 \mod 5 \\ \Rightarrow & 7 = 6 \cdot (2-1) + 1 \equiv 0 + 1 \equiv 1 \equiv x \mod 3 \\ \Rightarrow & 7 = 6 \cdot (2-1) + 1 \equiv 1 + 1 \equiv 2 \equiv x \mod 5 \\ & (3 \cdot 5) \equiv 15 \equiv 1 \mod 7 \\ & 7 \equiv 0 \mod 7 \\ \Rightarrow & 2 - 7 \equiv 2 \mod 7 \\ \Rightarrow & 37 = 15 \cdot 2 + 7 \equiv 15 \cdot (2-7) + 7 \equiv 7 \equiv 6 \cdot (2-1) + 1 \equiv 1 \equiv x \mod 3 \\ \Rightarrow & 37 = 15 \cdot 2 + 7 \equiv 15 \cdot (2-7) + 7 \equiv 7 \equiv 6 \cdot (2-1) + 1 \equiv 2 \equiv x \mod 5 \\ \Rightarrow & 37 = 15 \cdot 2 + 7 \equiv 15 \cdot (2-7) + 7 \equiv 2 \equiv x \mod 7 \end{aligned}$$

כלומר אני מסובב את גלגל השעון של 3 כדי לקבל 1 בשעון של 5 (קיבלנו 6), כעת אני בודק כמה אני צריך להוסיף ל-1 כדי לקבל את 2 (בשעון של 5) ומוסיף ל-1 את 6 (בשעון של 5) כפול ההפרש (קיבלנו 7); לאחר מכן אני מסובב את גלגל השעון של $3 \cdot 5$ כדי לקבל 1 בשעון של 7 (קיבלנו 15), כעת אני בודק כמה אני צריך להוסיף ל-7 כדי לקבל את 2 (בשעון של 7) ומוסיף ל-7 (בשעון של 7 שזה 0!) את 15 כפול ההפרש[4]. בכל שלב מובטח שהכול יהיה תקין מפני שאני מוסיף כפולות של כל המספרים שכבר עברתי, כך שאצלם אני לא משנה דבר, ובמספר שאני עובד עליו עכשיו אני מוסיף אחדות ולכן אוכל להגיע לאן שארצה.

מסקנה 1.15. יהיו $1 < m_1, m_2, \ldots, m_r \in \mathbb{N}$ זרים זה לזה בזוגות, יהיו $f_1, f_2, \ldots, f_r \in \mathbb{Z}[x]$ ויהיו $a_1, a_2, \ldots, a_r \in \mathbb{Z}$ כך ש-$f(a_i) \equiv 0 \mod m_i$ לכל $r \geq i \in \mathbb{N}$; קיים $n \in \mathbb{Z}$ כך ש-$f(n) \equiv 0 \mod m_i$ לכל $r \geq i \in \mathbb{N}$.

טענה 1.16. יהי $p \in \mathbb{N}$ מספר ראשוני, לכל $s \in \mathbb{N}$ מתקיים:

$$\phi(p^s) = p^s - p^{s-1} = p^{s-1} \cdot (p-1) = p^s \cdot \left(1 - \frac{1}{p}\right)$$

טענה 1.17. פונקציית אוילר כפלית עבור מספרים זרים[5], כלומר לכל $n, m \in \mathbb{N}$ הזרים זה לזה מתקיים $\phi(n \cdot m) = \phi(n) \cdot \phi(m)$.

הוכחה. הוכחה 1 - באמצעות הפונקציה שבהוכחה הראשונה של משפט השאריות הסיני
יהיו $n, m \in \mathbb{N}$ מספרים זרים זה לזה ותהא $f : (\mathbb{Z}/nm\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$ פונקציה המוגדרת ע"י (לכל $[x]_{nm} \in \mathbb{Z}/nm\mathbb{Z}$)[6]:

$$f([x]_{nm}) := ([x]_n, [x]_m)$$

[4] ניתן היה גם להתייחס ל-$7 - 2$ כ--5 ואז היינו מקבלים $-68 = 15 \cdot (-5) + 7 \equiv 37 \mod 105$ (והרי $105 = 3 \cdot 5 \cdot 7$).
[5] בהמשך, כשנלמד על פונקציות אריתמטיות, נקרא לפונקציה אריתמטית כזו כפלית סתם למרות שזו אינה ההגדרה הרגילה של פונקציה כפלית.
[6] הפונקציה מוגדרת היטב מפני שכל מספר זר ל-nm זר גם ל-n ו-m בנפרד.

ראינו בהוכחה הראשונה של משפט השאריות הסיני שזוהי פונקציה חח"ע[7], מצד שני זוהי גם פונקציה על מפני שלכל $(a,b) \in (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$ מתקיים:

$$f(bx \cdot n + ay \cdot m) = (ay \cdot m, bx \cdot n) = (a,b)$$

כאשר x,y הם שלמים המקיימים $1 = x \cdot n + y \cdot m$ ולכן גם $x \cdot n \equiv 1 \mod m$ ו-$y \cdot m \equiv 1 \mod n$.
מכאן שהתחום והטווח של f הן קבוצות באותו הגודל (שתיהן סופיות) וממילא:

$$\begin{aligned}\phi(n \cdot m) &= \left|(\mathbb{Z}/nm\mathbb{Z})^*\right| = \left|(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*\right| \\ &= \left|(\mathbb{Z}/n\mathbb{Z})^*\right| \cdot \left|(\mathbb{Z}/m\mathbb{Z})^*\right| = \phi(n) \cdot \phi(m)\end{aligned}$$

■

הוכחה. <u>הוכחה 2 - הכלה והדחה</u>
נוכיח את הטענה עבור מכפלת חזקות של שני ראשוניים שונים ואז מאינדוקציה תנבע המסקנה כולה.
יהיו $p,q \in \mathbb{N}$ שני ראשוניים שונים, מעיקרון ההכלה וההדחה[8] נובע שלכל $s,t \in \mathbb{N}$ מתקיים:

$$\phi\left(p^s \cdot q^t\right) = p^s \cdot q^t - p^{s-1} \cdot q^t - q^{t-1} \cdot p^s + p^{s-1} \cdot q^{t-1}$$

$$\begin{aligned}\Rightarrow \phi\left(p^s \cdot q^t\right) &= p^{s-1} \cdot q^{t-1} \cdot (p \cdot q - q - p + 1) \\ &= p^{s-1} \cdot q^{t-1} \cdot (p-1) \cdot (q-1) \\ &= p^{s-1} \cdot (p-1) \cdot q^{t-1} \cdot (q-1) \\ &= \phi(p^s) \cdot \phi\left(q^t\right)\end{aligned}$$

כעת נקבל מאינדוקציה שהטענה נכונה לכל מספר של ראשוניים שונים ומהקיבוץ של הכפל נקבל את הטענה עבור מספרים זרים באשר הם[9]. ■

מסקנה 1.18. יהי $n \in \mathbb{N}$ ויהיו $p_1, p_2, \ldots, p_r \in \mathbb{N}$ כל הראשוניים המחלקים את n ללא חזרות[10], מתקיים:

$$\phi(n) = \prod_{i=1}^{r}\left((p_i)^{\mathrm{Ord}_{p_i}(n)-1}\right) \cdot \prod_{i=1}^{r}(p_i - 1) = n \cdot \prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right)$$

♣ כדי להוכיח את נכונות המסקנה נשים לב לכך שדי להראות שהיא נכונה עבור חזקות של ראשוני כלשהו ואז מהכפליות של הפונקציה עבור מספרים זרים נקבל את הטענה עבור כל מספר, דרך זו תקפה לכל פונקציה כפלית עבור מספרים זרים.

מסקנה 1.19. יהי $n \in \mathbb{N}$, קיים $k \in \mathbb{N}_0$ כך ש-$\phi(n) = 2^k$ אם"ם כל הראשוניים האי-זוגיים בפירוק של n הם ראשוני פרמה והריבוי שלהם הוא 1.

[7] f בהוכחה שלנו היא צמצום של f בהוכחה הנ"ל לתת-הקבוצה $(\mathbb{Z}/nm\mathbb{Z})^* \subseteq \mathbb{Z}/nm\mathbb{Z}$ ולכן היא "יורשת" את תכונת החד-חד-ערכיות.
[8] $p^{s-1} \cdot q^t$ הוא מספר הכפולות של p הקטנות או שוות ל-$p^s \cdot q^t$, כמו כן $q^{t-1} \cdot p^s$ הוא מספר הכפולות של q בטווח זה ואילו $p^{s-1} \cdot q^{t-1}$ הוא כמות המספרים שהם כפולות של שניהם שהרי p ו-q זרים זה לזה ולכן כל כפולה של שניהם היא כפולה של $p \cdot q$.
[9] ראינו שניתן להציג כל מספר שלם כמכפלת חזקות של ראשוניים, וכמדובר בשני מספרים זרים הם אינם חולקים ראשוני משותף בפירוק.
[10] כלומר לכל $r \geq i,j \in \mathbb{N}$ מתקיים $p_i = p_j \iff i = j$.

1.3 משפטים נוספים

משפט 1.20. משפט וילסון (Wilson)[11]

יהי $p \in \mathbb{N}$ מספר ראשוני, מתקיים:

$$(p-1)! \equiv -1 \mod p$$

עבור $p=2$ המשפט טריוויאלי, נראה כעת שתי הוכחות עבור $p \neq 2$.

הוכחה. <u>הוכחה 1 - שימוש בתכונות השדה</u>

$\mathbb{Z}/p\mathbb{Z}$ הוא שדה ולכן מחלקות השקילות היחידות שהן ההופכיות של עצמן הן $\overline{1}$ ו-$\overline{p-1} = \overline{-1}$[12], א"כ לכל $i \in \mathbb{N}$ כך ש-$1 < i < p-1$ קיים $i \neq j \in \mathbb{N}$ כך ש-$1 < j < p-1$ ובנוסף $i \cdot j \equiv 1 \mod p$.

$$\Rightarrow (p-1)! \equiv (p-1) \cdot 1 \mod p$$
$$\Rightarrow (p-1)! \equiv p-1 \equiv -1 \mod p$$

<u>הוכחה 2 - שימוש בפירוק של פולינומים</u>

נתבונן בפולינום $f(x) := x^{p-1} - 1$ מעל ל-$\mathbb{Z}/p\mathbb{Z}$, מהמשפט הקטן של פרמה נובע שלכל $p > x \in \mathbb{N}$ מתקיים $x^{p-1} - 1 \equiv 0 \mod p$, כלומר ל-$f$ יש $p-1$ שורשים שונים ומכיוון שגם דרגתו היא $p-1$ הרי שהוא מתפרק למכפלת גורמים ליניאריים שונים:

$$f(x) = x^{p-1} - 1 = \prod_{i=1}^{p-1} (x-i)$$

ומכאן שמתקיים[13]:

$$(p-1)! \equiv \prod_{i=1}^{p-1} i \equiv (-1)^{p-1} \cdot \prod_{i=1}^{p-1} (-i) \equiv -1 \mod p$$

■

טענה 1.21. יהי $1 < n \in \mathbb{N}$, n הוא מספר ראשוני אם"ם $(n-1)! \equiv -1 \mod n$.

הוכחה. נוכיח את הכיוון ההפוך למשפט וילסון: נניח ש-$(n-1)! \equiv -1 \mod n$ ונניח בשלילה ש-n אינו ראשוני.
מכאן שקיים $a \in \mathbb{N}$ כך ש-$1 < a < n$ ו-$a \mid n$, מהגדרה אותו a מקיים $a \mid (n-1)!$ בסתירה לכך שע"פ טענה claim 1.3 מתקיים $(n-1)! \equiv -1 \mod a$, מכאן שהנחת השלילה אינה נכונה ו-n ראשוני. ■

משפט 1.22. יהי $2 < p \in \mathbb{N}$ מספר ראשוני, קיים $x \in \mathbb{Z}$ כך ש-$x^2 \equiv -1 \mod p$ אם"ם $p \equiv 1 \mod 4$.

הוכחה.

- $\Leftarrow$
  נניח שקיים $x \in \mathbb{Z}$ כך ש-$x^2 \equiv -1 \mod p$ ויהי x כנ"ל.
  מהמשפט הקטן של פרמה נובע שמתקיים:

$$1 \equiv x^{p-1} \equiv \left(x^2\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \mod p$$

---

[11] ערך בוויקיפדיה האנגלית: John Wilson.
[12] הוכחה: יהי $p > a \in \mathbb{N}$ ונניח ש-$a^2 \equiv 1 \mod p$, מכאן שמתקיים $(a+1)(a-1) \equiv a^2 - 1 \equiv 0 \mod p$ ולכן בהכרח מתקיים $a \equiv 1 \mod p$ ו/או ש-$a \equiv -1 \mod p$.
[13] המקדם החופשי של פולינום המתפרק לגורמים ליניאריים הוא מכפלת הנגדיים של השורשים.

אבל:

$$(-1)^{\frac{p-1}{2}}=\begin{cases}1 & \frac{p-1}{2}\in \text{Even}\\ -1 & \frac{p-1}{2}\in \text{Odd}\end{cases}=\begin{cases}1 & p\equiv 1 \mod 4\\ -1 & p\equiv 3 \mod 4\end{cases}$$

ומכיוון ש-$p\neq 2$ נדע ש-$1\not\equiv -1 \mod p$ ולכן בהכרח מתקיים $p\equiv 1 \mod 4$.

- $\Rightarrow$

נניח ש-$p\equiv 1 \mod 4$ ומכאן ש-$p-1\equiv 0 \mod 4$ וממילא $\frac{p-1}{2}\equiv 0 \mod 2$, כלומר $\frac{p-1}{2}\in \text{Even}$ ו-$(-1)^{\frac{p-1}{2}}=1$.
ממשפט וילסון נובע שמתקיים:

$$\begin{aligned}-1\equiv (p-1)!\equiv \prod_{i=1}^{p-1} i &\equiv \left(\prod_{i=\frac{p-1}{2}+1}^{p-1} i\right)\cdot\left(\prod_{i=1}^{\frac{p-1}{2}} i\right)\equiv\left(\prod_{i=1}^{\frac{p-1}{2}} -i\right)\cdot\left(\prod_{i=1}^{\frac{p-1}{2}} i\right)\\ &\equiv (-1)^{\frac{p-1}{2}}\cdot\left(\prod_{i=1}^{\frac{p-1}{2}} i\right)\cdot\left(\prod_{i=1}^{\frac{p-1}{2}} i\right)\equiv\left(\prod_{i=1}^{\frac{p-1}{2}} i\right)^2 \mod p\end{aligned}$$

כלומר קיים $x\in\mathbb{Z}$ כך ש-$x^2\equiv -1 \mod p$.

■

טענה 1.23. קיימים אינסוף ראשוניים השקולים ל-1 מודולו 4, כלומר הקבוצה $\{p\in \text{Prime} \mid p\equiv 1 \mod 4\}$ היא קבוצה אינסופית.

הוכחה. נניח בשלילה מספר הראשוניים השקולים ל-1 מודולו 4 הוא סופי ויהיו $p_1,p_2,\ldots,p_r\in\mathbb{N}$ כל הראשוניים הללו, נסמן:

$$m:=\prod_{i=1}^{r}(p_i)^2,\ \ n:=4m+1$$

יהי $p\in\mathbb{N}$ ראשוני המחלק את n, מהגדרה מתקיים $4m\equiv -1 \mod p$; נשים לב לכך שמתקיים:

$$4m=\left(2\cdot\prod_{i=1}^{r}p_i\right)^2$$

ולכן קיים $x\in\mathbb{Z}$ כך ש-$x^2\equiv -1 \mod p$ ומכאן שע"פ המשפט האחרון מתקיים $p\equiv 1 \mod 4$.
אבל מהגדרה p אינו אחד מן הראשוניים הנ"ל (שהרי p_i אינו מחלק את n לכל $r\geq i\in\mathbb{N}$) וזאת בסתירה לכך שאלו כל הראשוניים השקולים ל-1 מודולו 4, מכאן שהנחת השלילה אינה נכונה וקיימים אינסוף ראשוניים השקולים ל-1 מודולו 4. ■

טענה 1.24. קיימים אינסוף ראשוניים השקולים ל-3 מודולו 4, כלומר הקבוצה $\{p\in \text{Prime} \mid p\equiv 3 \mod 4\}$ היא קבוצה אינסופית.

הוכחה. נניח בשלילה מספר הראשוניים השקולים ל-1 מודולו 4 הוא סופי ויהיו $p_1,p_2,\ldots,p_r\in\mathbb{N}$ כל הראשוניים הללו, נסמן:

$$m:=\prod_{i=1}^{r}p_i,\ \ n:=4m-1$$

נשים לב לכך ש-$n\equiv 3 \mod 4$ ולכן בהכרח קיים ראשוני השקול ל-3 מודולו 4 המחלק את n, שהרי n אי-זוגי ומכפלה של ראשוניים השקולה ל-1 מודולו 4 תהיה גם היא שקולה ל-1 מודולו 4.
א"כ יהי $p\in\mathbb{N}$ ראשוני המחלק n כך ש-$p\equiv 3 \mod 4$, מהגדרה p אינו אחד מן הראשוניים הנ"ל (שהרי p_i אינו מחלק את n לכל $r\geq i\in\mathbb{N}$) וזאת בסתירה לכך שאלו כל הראשוניים השקולים ל-3 מודולו 4, מכאן שהנחת השלילה אינה נכונה וקיימים אינסוף ראשוניים השקולים ל-3 מודולו 4. ■

♣ הטענות בעצם אומרות שבסדרות $(4n+1)_{n=0}^{\infty}$ ו-$(4n+3)_{n=0}^{\infty}$ יש אינסוף ראשוניים ובכך הן מקרה פרטי של משפט דיריכלה שראינו בנושא הקודם: לכל $a,d\in\mathbb{N}$ הזרים זה לזה קיימים אינסוף איברים ראשונים שהם איברים בסדרה החשבונית $(a+dn)_{n=0}^{\infty}$.

משפט 1.25. יהיו $A\in M_{n}\left(\mathbb{Z}/N\mathbb{Z}\right)$ ו-$b\in\left(\mathbb{Z}/N\mathbb{Z}\right)^{n}$, למערכת המשוואות הליניאריות $A\cdot x\equiv b\mod N$[14] יש פתרון יחיד אם"ם $\overline{\det A}\in\left(\mathbb{Z}/N\mathbb{Z}\right)^{*}$, כלומר אם"ם הדטרמיננטה של A היא מספר זר ל-N, אחרת ייתכן שאין פתרונות כלל או שיש יותר מפתרון אחד.

♣ נזכיר שכדי לפתור מערכות משוואות ליניאריות (ממ"ל) מעל שדה ראינו בליניארית 1 את אלגוריתם הדירוג (דירוג מטריצות) המשתמש בשלוש פעולות שורה אלמנטריות (פש"א): החלפת שורות, כפל שורה בסקלר מהשדה והוספת כפולה של שורה אחת לשורה אחרת; כשמבצעים את האלגוריתם מעל חוג שלמים מודולרי $\mathbb{Z}/N\mathbb{Z}$ יש להיזהר בשתי הפעולות האחרונות: לא לכל סקלר בחוג יש הופכי, זה הורס את האלגוריתם וכבר א"א לבצעו בצורה מכנית[15] ויש לחשוב במהלך הדירוג.

♣ ההוכחה של המשפט משתמשת בכלל קרמר ובלמה שקדמה לו (ראו בקובץ "פונקציות נפח - טענות בלבד"), זוכרים שחשבנו שהוא מיותר לחלוטין מפני שאלגוריתם הדירוג הרבה יותר יעיל? אז הנה שימוש שלו.

הוכחה. בליניארית 1 ראינו את הלמה הבאה:

למה. תהא $M\in M_{n}\left(\mathbb{F}\right)$ מטריצה ($\mathbb{F}$ הוא שדה), יהי $v\in\mathbb{F}^{n}$ ונסמן ב-$M^{(i)}$ את המטריצה המתקבלת מ-M ע"י החלפת העמודה ה-i ב-v (לכל $n\geq i\in\mathbb{N}$).
אם קיים $x\in\mathbb{F}^{n}$ כך ש-$M\cdot x=v$ אז עבור אותו x מתקיים (לכל $n\geq i\in\mathbb{N}$):

$$\det M^{(i)}=\left(\det M\right)\cdot x_{i}$$

נניח שקיים $x\in\mathbb{Z}^{n}$ כך ש-$A\cdot x\equiv b\mod N$ ויהי x כנ"ל. נסתכל על A כמטריצה ב-$M_{n}\left(\mathbb{Q}\right)$, א"כ גם A מקיימת $\det A^{(i)}=\left(\det A\right)\cdot x_{i}$ (לכל $n\geq i\in\mathbb{N}$)[16].
כעת נשים לב לכך שכל הרכיבים ב-A וב-$A^{(i)}$ הם מספרים שלמים, ולכן מהנוסחה המפורשת של הדטרמיננטה נובע שגם $\det A$ ו-$\det A^{(i)}$ הם מספרים שלמים; מכאן שלכל $n\geq i\in\mathbb{N}$ מתקיים:

$$\det A^{(i)}\equiv\left(\det A\right)\cdot x_{i}\mod N$$

בהערה על משפט 1.6 ראינו שאם $\det A$ אינו זר ל-N וגם יש פתרונות מודולו N, אז יש יותר מפתרון אחד (כי $\gcd\left(\det A,N\right)>1$); א"כ הוכחנו שאם קיים פתרון יחיד אז $\overline{\det A}\in\left(\mathbb{Z}/N\mathbb{Z}\right)^{*}$.
בנוסף, ניתן לראות כבר כעת שאם $\overline{\det A}\in\left(\mathbb{Z}/N\mathbb{Z}\right)^{*}$ וגם יש פתרון מודולו N אז הפתרון יחיד, א"כ נשאר לנו להוכיח שאם $\overline{\det A}\in\left(\mathbb{Z}/N\mathbb{Z}\right)^{*}$ אז קיים פתרון.
נניח ש-$\overline{\det A}\in\left(\mathbb{Z}/N\mathbb{Z}\right)^{*}$, בפרט $\det A\neq0$ ולכן מכלל קרמר נובע שלכל $n\geq i\in\mathbb{N}$ מתקיים (מעל $\mathbb{Q}$):

$$\frac{1}{\det A}\cdot\sum_{k=1}^{n}\left[A\right]_{ik}\cdot\det A^{(k)}=b_{k}$$

כלומר:

$$\sum_{k=1}^{n}\left[A\right]_{ik}\cdot\det A^{(k)}=\left(\det A\right)\cdot b_{k}$$

וזהו כבר שוויון ב-$\mathbb{Z}$ ולכן נקבל:

$$A\cdot\begin{bmatrix}\det A^{(1)}\\
\det A^{(2)}\\
\vdots\\
\det A^{(n)}
\end{bmatrix}\equiv\left(\det A\right)\cdot b\mod N$$

[14] הכוונה היא שהווקטורים בשני האגפים מחושבים מעל $\mathbb{Z}$ ומתקיימת שקילות מודולו N בכל קואורדינטה.
[15] אולי ניתן לתקן אותו אך כפי שלמדנו אותו הוא כבר לא עובד משום שהוא השתמש בכפל בהופכי ע"מ לייצר אחדות מובילים.
[16] נסמן ב-$A^{(i)}$ את המטריצה המתקבלת מ-A ע"י החלפת העמודה ה-i ב-b (לכל $n\geq i\in\mathbb{N}$).

מההנחה ש-$\overline{\det A} \in (\mathbb{Z}/N\mathbb{Z})^*$ נובע שיש ל-$\det A$ הופכי מודולו N ועבורו מתקיים:

$$A \cdot \begin{bmatrix} (\det A)^{-1} \cdot \det A^{(1)} \\ (\det A)^{-1} \cdot \det A^{(2)} \\ \vdots \\ (\det A)^{-1} \cdot \det A^{(n)} \end{bmatrix} \equiv b \mod N$$

■

משפט 1.26. יהיו $a, b, c \in \mathbb{Z}$, לקונגרואנציה $ax^2 + bx + c \equiv 0 \mod N$ יש פתרון אם"ם $2a \in (\mathbb{Z}/N\mathbb{Z})^*$ ו-$b^2 - 4ac$ הוא שארית ריבועית מודולו N ובמקרה כזה כל $d \in \mathbb{Z}$ כך ש-$d^2 \equiv b^2 - 4ac \mod N$ נותן פתרון שהוא:

$$x \equiv (-b + d) \cdot (2a)^{-1} \mod N$$

♣ נשים לב לכך שמדובר בנוסחת השורשים שהרי d הוא $\sqrt{b^2 - 4ac}$ ואז $(-b + d) \cdot (2a)^{-1}$ הוא בעצם:

$$\frac{-b + \sqrt{b^2 - 4ac}}{2a}$$

שימו לב שההערה הזו ממש לא פורמלית, הביטוי $\sqrt{b^2 - 4ac}$ אינו מוגדר שהרי ייתכן שלשארית ריבועית יש יותר משורש אחד.

♣ הדמיון לנוסחת השורשים אינו מקרי כמובן, ההוכחה של נוסחת השורשים תעבוד גם כאן אלא שעלינו לשים לב לכך שאנו מוציאים שורש של $b^2 - 4ac$ ומחלקים ב-$2a$, כלומר הפעולות הללו צריכות להיות מוגדרות כדי שיהיה פתרון ומכאן נובעים התנאים הנ"ל.

משפט 1.27. הלמה של הנזל[17]

יהי $f\in\mathbb{Z}[x]$ פולינום ויהיו $p,e\in\mathbb{N}$ כך ש-p ראשוני, אם קיים $a\in\mathbb{Z}$ כך ש-$f(a)\equiv 0\mod p^{e}$ ו-$f'(a)\not\equiv 0\mod p$[18] אז קיים $b\in\mathbb{Z}$ כך ש-$b\equiv a\mod p^{e}$ וגם $f(b)\equiv 0\mod p^{e+1}$[19]; בנוסף, אותו b הוא יחיד מודולו p^{e+1}, כלומר לכל $c\in\mathbb{Z}$ המקיים $c\equiv a\mod p^{e}$ וגם $f(c)\equiv 0\mod p^{e+1}$ מתקיים $c\equiv b\mod p^{e+1}$.

הפתרון שמביאה הוכחת המשפט הוא (לכל $t\in\mathbb{Z}$ המקיים את השקילות שלהלן):

$$b=a+t\cdot p^{e},\ \ t\equiv -f'(a)^{-1}\cdot\frac{f(a)}{p^{e}}\mod p$$

ומכאן הדרישה שיתקיים $f'(a)\not\equiv 0\mod p$.

הוכחה. נסמן $n:=\deg f$, ראינו באינפי' 1 בפרק על פולינומי טיילור שלכל $a\in\mathbb{R}$ מתקיים[20]:

$$P_{n,f,a}(x)=f(x)$$

בפרט הדבר נכון עבור $a\in\mathbb{Z}$ המקיים $f(a)\equiv 0\mod p^{e}$, נניח שאכן יש ל-f שורש מודולו p^{e} ויהי $a\in\mathbb{Z}$ שורש כזה. כעת נשים לבל לכך שלכל $t\in\mathbb{Z}$ מתקיים:

$$f(a+t\cdot p^{e})=P_{n,f,a}(a+t\cdot p^{e})=\sum_{k=0}^{n}\frac{f^{(k)}(a)}{k!}\cdot(a+t\cdot p^{e}-a)^{k}=\sum_{k=0}^{n}\frac{f^{(k)}(a)}{k!}\cdot(t\cdot p^{e})^{k}$$

אך לכל $2\le k\in\mathbb{N}$ מתקיים $(t\cdot p^{e})^{k}\equiv t^{k}\cdot p^{e\cdot k}\equiv 0\mod p^{e+1}$ ומכאן נובע כי לכל $t\in\mathbb{Z}$ מתקיים:

$$f(a+t\cdot p^{e})=\sum_{k=0}^{n}\frac{f^{(k)}}{k!}\cdot(t\cdot p^{e})^{k}\equiv f(a)+f'(a)\cdot t\cdot p^{e}\mod p^{e+1}$$

מהגדרה $f(a)\equiv 0\mod p^{e}$, א"כ קיים $k\in\mathbb{Z}$ כך ש-$f(a)=k\cdot p^{e}$, יהי k כנ"ל ($k:=\frac{f(a)}{p^{e}}$) ומכאן שמתקיים:

$$f(a+t\cdot p^{e})\equiv p^{e}\cdot(k+f'(a)\cdot t)\mod p^{e+1}$$

כעת, אם $f'(a)\not\equiv 0\mod p$ אז יש ל-$f'(a)$ הופכי מודולו p ואותו הופכי מקיים:

$$f(a+t\cdot p^{e})\equiv 0\mod p^{e+1}\iff k+f'(a)\cdot t\equiv 0\mod p$$

$$\iff t\equiv -f'(a)^{-1}\cdot k\equiv -f'(a)^{-1}\cdot\frac{f(a)}{p^{e}}\mod p$$

אנחנו יודעים שלכל שורש $b\in\mathbb{Z}$ של f מודולו p^{e+1} קיים $t\in\mathbb{Z}$ כך ש-$b\equiv a+t\cdot p^{e}\mod p^{e+1}$ ולכן השורה הקודמת מראה הן את הקיום של t כזה והן את יחידותו מודולו p, יחידות זו נותנת גם את היחידות של מודולו p^{e+1} מפני שלכל $t_1,t_2\in\mathbb{Z}$ כך ש-$t_1\equiv t_2\mod p$ (כלומר $p\mid t_1-t_2$) מתקיים גם $t_1\cdot p^{e}\equiv t_2\cdot p^{e}$ (כלומר $p^{e+1}\mid(t_1-t_2)\cdot p^{e}$). ■

♣ הלמה של הנזל, יחד עם משפט השאריות הסיני, נותנים לנו דרך מצוא שורשים של פולינומים בכל מודולוס ובתנאי שאנחנו יודעים את השורשים של הפולינום עבור כל אחד מהראשוניים המופיעים בפירוק של המודולוס.

♣ בוויקיפדיה מופיעה הרחבה ללמה של הנזל העוסקת במקרה שבו $f'(a)\equiv 0\mod p$:

- אם $f'(a)\equiv 0\mod p$ וגם $f(a)\equiv 0\mod p^{e+1}$ אז $f(a+t\cdot p^{e})\equiv 0\mod p^{e+1}$ לכל $t\in\mathbb{Z}$.
- אם $f'(a)\equiv 0\mod p$ וגם $f(a)\not\equiv 0\mod p^{e+1}$ אז לא קיים $t\in\mathbb{Z}$ כך ש-$f(a+t\cdot p^{e})\equiv 0\mod p^{e+1}$, כלומר אין ל-$f$ שורשים מודולו p^{e+1}.

♣ a כנ"ל נקרא "שורש פשוט" של הפולינום, כלומר שורש פשוט הוא מספר שהצבתו בפולינום נותנת 0 אבל הצבתו בפולינום הנגזרת שונה מ-0.

---

[17] ערך בוויקיפדיה: קורט הנזל.

[18] פולינום הנגזרת של פולינום בעל מקדמים שלמים שייך גם הוא לחוג הפולינומים מעל השלמים.

[19] נשים לב לכך שמכיוון ש-$a\equiv b\mod p$ נקבל גם $f'(b)\equiv f'(a)\not\equiv 0\mod p$ ולכן ניתן להמשיך ו"להעלות" פתרונות עד לחזקה הרצויה.

[20] פולינום טיילור של פולינום, מסדר שווה לדרגת הפולינום, שווה לו עצמו בכל נקודה.

2 פונקציות אריתמטיות

טענה 2.1. מתקיים $\delta, I_k, \sigma_k\phi, \mu, S \in \mathcal{M}$ (לכל $k \in \mathbb{N}_0$), כלומר כל הפונקציות שראינו הן פונקציות כפליות.

♣ מכיוון שכבר ראינו ש-$S(p) = \frac{p+1}{2}$ לכל $2 < p \in \mathbb{N}$ ראשוני (ו-$S_2 = 2$) נוכל לחשב את הערך של $S(n)$ לכל n חופשי מריבועים.

משפט 2.2. לכל $f, g, h \in \mathcal{F}$ מתקיימים כל הפסוקים הבאים:

1. $f * g = g * f$ - הקונבולציה קומוטטיבית.
2. $f * (g * h) = (f * g) * h$ - הקונבולוציה אסוציאטיבית.
3. $f * (g + h) = f * g + f * h$ - הקונבולוציה דיסטריבוטיבית ביחס לחיבור.
4. $f * \delta = f$
5. אם f ו-g כפליות אז גם $f * g$ כפלית.
6. $\mu * I_0 = \delta$.
7. נוסחת ההיפוך של מביוס: אם $g(n) = \sum_{0<d|n} f(d)$ (לכל $n \in \mathbb{N}$) אז $f(n) = \sum_{0<d|n} g(d) \cdot \mu\left(\frac{n}{d}\right)$ (לכל $n \in \mathbb{N}$), ניתן לראות זאת גם כך: אם $g = f * I_0$ אז $f = g * \mu$.

טענה 2.3. מתקיים $\phi * I_0 = I_1$, כלומר לכל $n \in \mathbb{N}$ מתקיים:

$$\sum_{0<d|n} \phi(d) = \sum_{0<d|n} \phi(d) \cdot I_0\left(\frac{n}{d}\right) = (\phi * I_0)(n) = I_1(n) = n$$

הוכחה. נוכיח (באינדוקציה) שהטענה נכונה עבור חזקות של ראשוניים ומהכפליות של הקונבולוציה $\phi * I_0$ ינבע שהטענה נכונה לכל מספר.

יהי $p \in \mathbb{N}$ ראשוני, מהגדרה מתקיים:

$$\sum_{0<d|p} \phi(d) = \phi(1) + \phi(p) = 1 + (p-1) = p$$

נניח באינדוקציה שהטענה נכונה עבור p^e ונוכיח עבור p^{e+1}, המחלקים של p^{e+1} הם המחלקים של p^e יחד עם p^{e+1} עצמו.

$$\Rightarrow \sum_{0<d|p^{e+1}} \phi(d) = \phi\left(p^{e+1}\right) - \sum_{0<d|p^e} \phi(d) = \left(p^{e+1} - p^e\right) + p^e = p^{e+1}$$

■

מסקנה 2.4. מתקיים $\phi = I_1 * \mu$, כלומר לכל $n \in \mathbb{N}$ מתקיים:

$$\phi(n) = \sum_{0<d|n} I_1(d) \cdot \mu\left(\frac{n}{d}\right) = \sum_{0<d|n} d \cdot \mu\left(\frac{n}{d}\right)$$

טענה 2.5. שקילויות נוספות, מתקיים:

1. $\sigma_0 = I_0 * I_0$
2. $\sigma_1 = I_1 * I_0$

מסקנה 2.6. מתקיים $\sigma_1 = \phi * \sigma_0$[21].

הוכחה. ממסקנה 2.4 ומטענה 2.5 נובע שמתקיים:

$$\sigma_1 = I_1 * I_0 = I_1 * \delta * I_0 = (I_1 * \mu) * (I_0 * I_0) = \phi * \sigma_0$$

■

3 שורשים פרימיטיביים

יהי $1 < N \in \mathbb{N}$.

טענה 3.1. לכל $\overline{a} \in (\mathbb{Z}/N\mathbb{Z})^*$ מתקיים $e_N(a) \mid \phi(N)$.

טענה 3.2. לכל $a \in \mathbb{Z}$ זר ל-N ולכל $i, j \in \mathbb{N}$[22], מתקיים $a^i \equiv a^j \mod N$ אם"ם $i \equiv j \mod e_N(a)$.

♣ הטענה מראה לנו שמההגדרה נובע שכדי לחשב חזקות בחשבון מודולו N ניתן לבצע חשבון מודולו $e_N(a)$ על המעריך וזאת בתנאי שהבסיס זר ל-N.

♣ בפרט לכל שורש פרימיטיבי $a \in \mathbb{Z}$ של N מתקיים (לכל $i \in \mathbb{N}$) $a^i \equiv 1 \mod N$ אם"ם $i \equiv 0 \mod \phi(N)$, כלומר אם"ם $\phi(N) \mid i$.

מסקנה 3.3. לכל שורש פרימיטיבי a של N מתקיים $\left\{a^k \mid k \in \mathbb{N}\right\} = (\mathbb{Z}/N\mathbb{Z})^*$.

למה 3.4. יהי $p \in \mathbb{N}$ ראשוני, ויהי $p - 1 \geq d \in \mathbb{N}$ כך ש-$d \mid p - 1$, לפולינום $x^d - 1$ (מעל $\mathbb{Z}/p\mathbb{Z}$) יש d שורשים.

הוכחה. נסמן $q := \frac{p-1}{d}$ ונשים לב לכך שמתקיים:

$$x^{p-1} - 1 = \left(x^d\right)^q - 1 = \left(x^d - 1\right) \cdot \sum_{k=0}^{q-1} \left(x^d\right)^{q-1-k}$$

כעת, מכיוון של-$x^{p-1} - 1$ יש $p - 1$ שורשים (המשפט הקטן של פרמה) נדע של-$x^d - 1$ יש d שורשים שהרי דרגת הפולינום הימני במכפלה היא $(q-1) \cdot d = q \cdot d - d = p - 1 - d$ ולכן יש לו לכל היותר $p - 1 - d$ שורשים. ■

למה 3.5. יהי $n \in \mathbb{N}$, נסמן ב-D את קבוצת המחלקים הטבעיים של n ותהיינה $f, g : D \to \mathbb{C}$[23], אם לכל $d \in D$ מתקיים $\sum_{0<e|d} f(e) = \sum_{0<e|d} g(e)$ אז $f = g$.

הוכחה. נניח בשלילה שקיים $d \in D$ כך ש-$f(d) \neq g(d)$ ויהי d האיבר המינימלי המקיים זאת, א"כ לכל מחלק $d > e \in \mathbb{N}$ של n מתקיים $f(e) = g(e)$.

נתון כי $\sum_{0<e|d} g(d) = \sum_{0<e|d} f(d)$ ומכאן שע"פ השורה הקודמת מתקיים $f(d) = g(d)$ בסתירה להגדרת d, א"כ הנחת השלילה אינה נכונה ולכל $d \in D$ מתקיים $f(d) = g(d)$. ■

---

[21] שימו לב לדמיון בין $\phi * I_0 = I_1$ ל-$\phi * \sigma_0 = \sigma_1$.

[22] למעשה ניתן היה לכתוב "לכל $i, j \in \mathbb{Z}$" וכן במסקנות מהמשפט הקטן של פרמה וממשפט אוילר אבל לא התעסקנו בחזקות שאינן טבעיות בקורס.

[23] נשים לב ש-f ו-g אינן מוגדרות על כל הטבעיים ולכן א"א להשתמש בנוסחת ההיפוך של מביוס.

משפט 3.6. יהי $p\in\mathbb{N}$ ראשוני, לכל $p>d\in\mathbb{N}$ המחלק את $p-1$ מתקיים $\phi\left(d\right)=\left|\left\{ \overline{a}\in\mathbb{Z}/p\mathbb{Z}\mid e_{p}\left(a\right)=d\right\} \right|$, כלומר לכל $d\in\mathbb{N}$ כך ש-$d\mid p-1$ קיימים $\phi\left(d\right)$ איברים בשדה $\mathbb{F}_{p}$ שהמעריך שלהם הוא d.

הוכחה. נסמן ב-D את קבוצת המחלקים הטבעיים של $p-1$ ותהא $\omega:D\rightarrow\mathbb{N}_{0}$ פונקציה המוגדרת ע"י (לכל $d\in D$):

$$\omega\left(d\right):=\left|\left\{ \overline{a}\in\mathbb{Z}/p\mathbb{Z}:e_{p}\left(a\right)=d\right\} \right|$$

ראינו בלמה 3.4 שלפולינום $x^{d}-1$ יש בדיוק d שורשים לכל $d\in D$, בנוסף אנחנו יודעים שלכל $a\in\mathbb{Z}$ כך ש-$a^{d}-1\equiv0\mod p$ מתקיים $e_{p}\left(a\right)\mid d$; מכאן שלכל $d\in D$ מתקיים:

$$d=\sum_{0<e\mid d}\omega\left(e\right)$$

ולכן ע"פ למה 3.5 וטענה 2.3 מתקיים $\phi\left(d\right)=\omega\left(d\right)=\left|\left\{ \overline{a}\in\mathbb{Z}/p\mathbb{Z}:e_{p}\left(a\right)=d\right\} \right|$ לכל $d\in D$.[24] ■

♣ בפרט, לכל $p\in\mathbb{N}$ ראשוני קיימים $\phi\left(p-1\right)$ שורשים פרימיטיביים.

למה 3.7. יהיו $2<p\in\mathbb{N}$ ראשוני ו-$t\in\mathbb{N}$, ויהיו $a,b\in\mathbb{Z}$ כך ש-a ו-b אינם מתחלקים ב-p, אם $a\not\equiv b\mod p^{t}$ אז $a^{p}\not\equiv b^{p}\mod p^{t+1}$.

הוכחה. נניח ש-$a\not\equiv b\mod p^{t}$ ונסמן $s:=\max\left\{ i\in\mathbb{N}_{0}:p^{s}\mid a-b\right\}$, אם $s=0$ אז $a\not\equiv b\mod p$ ולכן מהמשפט הקטן של פרמה נובע שגם $a^{p}\not\equiv b^{p}\mod p$ וממילא גם $a^{p}\not\equiv b^{p}\mod p^{t+1}$.
אחרת $s\geq1$ וקיים $k\in\mathbb{Z}$ שאינו מתחלק ב-p כך ש-$a=b+k\cdot p^{s}$, יהי k כנ"ל.

$$\begin{aligned}\Rightarrow a^{p} & =\sum_{i=0}^{p}\binom{p}{i}\cdot b^{p-i}\cdot\left(k\cdot p^{s}\right)^{i}\\
 & =b^{p}+p\cdot b^{p-1}\cdot k\cdot p^{s}+\binom{p}{2}\cdot b^{p-2}\cdot k^{2}\cdot p^{2s}+\sum_{i=2}^{p}\binom{p}{i}\cdot b^{p-i}\cdot k^{i}\cdot p^{s\cdot i}\\
 & \equiv b^{p}+p\cdot b^{p-1}\cdot k\cdot p^{s}+\binom{p}{2}\cdot b^{p-2}\cdot k^{2}\cdot p^{2s}\mod p^{s+2}
\end{aligned}$$

נשים לב לכך שמתקיים $\binom{p}{2}=\frac{p\cdot\left(p-1\right)}{2}\mid p$[25] ומכאן שגם $p^{s+2}\mid\binom{p}{2}\cdot b^{p-2}\cdot k^{2}\cdot p^{2s}$.

$$\Rightarrow a^{p}\equiv b^{p}+p\cdot b^{p-1}\cdot k\cdot p^{s}\mod p^{s+2}$$

נזכור ש-p אינו מחלק את b ואת k ומכאן ש-$p\cdot b^{p-1}\cdot k\cdot p^{s}\not\equiv0\mod p^{s+2}$ וממילא $a^{p}\not\equiv b^{p}\mod p^{s+2}$. מהגדרה $t\geq s+1$ ולכן $t+1\geq s+2$ ומכאן ש-$a^{p}\not\equiv b^{p}\mod p^{t+1}$. ■

טענה 3.8. יהיו $2<p\in\mathbb{N}$ ראשוני ו-$a\in\mathbb{Z}$ שורש פרימיטיבי של p, אם $a^{p-1}\not\equiv1\mod p^{2}$ אז a הוא שורש פרימיטיבי של p^{e} לכל $e\in\mathbb{N}$, ואם $a^{p-1}\equiv1\mod p^{2}$ אז $a+p$ הוא שורש פרימיטיבי של p^{e} לכל $e\in\mathbb{N}$.

הוכחה. נסמן $x:=e_{p^{2}}\left(a\right)$, א"כ $a^{x}\equiv1\mod p^{2}$ וממילא גם $a^{x}\equiv1\mod p$ ולכן מהיות a שורש פרימיטיבי של p נובע ש-$p-1\mid x$ (טענה 3.2), מצד שני מטענה 3.1 נדע שמתקיים $x\mid\phi\left(p^{e}\right)=p^{e-1}\cdot\left(p-1\right)$ ולכן:

1. אם $a^{p-1}\not\equiv1\mod p^{2}$ אז $x\neq p-1$ ולכן (בגלל ש-$e\mid p\cdot\left(p-1\right)$ וגם $p-1\mid e$[26]) מתקיים בהכרח $e=p\cdot\left(p-1\right)=\phi\left(p^{2}\right)$, כלומר a הוא שורש פרימיטיבי של p^{2}.

---

[24] למעשה למה 3.5 אומרת ש-$\phi\mid_{D}$ (הצמצום של ϕ ל-D) שווה ל-ω.
[25] נזכור ש-$p>2$.
[26] הנימוק הזה הוא שאינו עובד במקרה שבו $p=2$: זה $2\mid e$ וגם $e\mid1$ לא אומר ש-$e=2$, ייתכן ש-$e=1$.

2. אם $a^{p-1}\equiv 1 \mod p^2$ אז מכיוון שמתקיים:

$$\begin{aligned}(a+p)^{p-1}&=\sum_{i=0}^{p-1}\binom{p-1}{i}\cdot a^{p-1-i}\cdot p^i=a^{p-1}+(p-1)\cdot a^{p-2}\cdot p+\sum_{i=2}^{p-1}\binom{p-1}{i}\cdot a^{p-1-i}\cdot p^i\\&\equiv a^{p-1}+(p-1)\cdot a^{p-2}\cdot p\equiv a^{p-1}-a^{p-2}\cdot p\not\equiv 1 \mod p^2\end{aligned}$$

ובנוסף $e_p(a+p)=e_p(a)=p-1$ נדע ש-$p-1\mid e_{p^2}(a+p)$ ולכן מאותן סיבות שבסעיף הקודם מתקיים בהכרח $e_{p^2}(a+p)=p\cdot(p-1)$ ו-$a+p$ הוא שורש פרימיטיבי של p^2.

כעת נוכיח באינדוקציה שכל שורש פרימיטיבי מודולו p^2 הוא גם שורש פרימיטיבי של p^e לכל $2<e\in\mathbb{N}$.

יהי $2\le e\in\mathbb{N}$, יהי $b\in\mathbb{Z}$ שורש פרימיטיבי של p^e, א"כ מתקיים $b^{p^{e-2}\cdot(p-1)}\not\equiv 1 \mod p^e$, ולכן ע"פ למה 3.7 מתקיים $b^{p^{e-1}\cdot(p-1)}\not\equiv 1 \mod p^{e+1}$.

מצד שני מטענה 3.2 נובע שמתקיים $p-1\mid e_{p^{e+1}}(b)$ ומטענה 3.1 מתקיים $e_{p^{e+1}}(b)\mid\phi\left(p^{e+1}\right)=p^e\cdot(p-1)$ ועל כן בהכרח:

$$e_{p^{e+1}}(b)=p^e\cdot(p-1)$$

כלומר b הוא שורש פרימיטיבי מודולו p^{e+1}. ■

טענה 3.9. יהיו $2<p\in\mathbb{N}$ ראשוני, $k\in\mathbb{N}$ ו-$a\in\mathbb{Z}$ שורש פרימיטיבי של p^k[27], המספר האי-זוגי מבין a ו-$a+p^k$[28] הוא שורש פרימיטיבי של $2p^k$.

הוכחה. ראשית נבחין שהדרישה לאי-זוגיות נובעת מהצורך הבסיסי שהשורש יהיה זר ל-$2p^k$ ובפרט זר ל-2, נסמן את האי-זוגי מבין a ו-$a+p^k$ ב-b.

מטענה 3.2 נובע שמתקיים:

$$e_{p^k}(b)\mid e_{2p^k}(b),\ \ e_{2p^k}(b)\mid\phi\left(2p^k\right)$$

אבל לכל $m\in\text{Odd}$ מתקיים $\phi(2m)=\phi(m)$ ובפרט $\phi\left(2p^k\right)=\phi\left(p^k\right)$.

כעת נזכור ש-b הוא שורש פרימיטיבי מודולו p^k ועל כן $e_{p^k}(b)=\phi\left(p^k\right)=\phi\left(2p^k\right)$ ומכאן שמתקיים:

$$\phi\left(2p^k\right)\mid e_{2p^k}(b)$$

ולכן בהכרח:

$$e_{2p^k}(b)=\phi\left(2p^k\right)$$

כלומר b הוא שורש פרימיטיבי מודולו $2p^k$. ■

טענה 3.10. אם N מתחלק בשני ראשוניים אי-זוגיים שונים אז אין ל-N שורש פרימיטיבי.

הוכחה. נניח ש-N מתחלק בשני ראשוניים אי-זוגיים שונים ויהיו $n,m\in\mathbb{N}$ זרים זה לזה כך ש-$N=n\cdot m$ ולשניהם יש מחלק ראשוני אי-זוגי.

נסמן $l:=\text{lcm}\left(\phi(n),\phi(m)\right)$, מהגדרה מתקיים $l\mid\phi(n)$ וגם $l\mid\phi(m)$ ולכן ממשפט אוילר נובע שלכל $\overline{a}\in(\mathbb{Z}/N\mathbb{Z})^*$ מתקיים:

$$a^l\equiv 1 \mod n$$
$$a^l\equiv 1 \mod m$$

ומכאן שע"פ משפט השאריות הסיני מתקיים גם $a^l\equiv 1 \mod N$[29].

כעת נשים לב לכך ש-$\phi(n),\phi(m)\in\text{Even}$ ולכן בהכרח $l<\phi(n)\cdot\phi(m)=\phi(N)$ ומכאן שלכל $\overline{a}\in(\mathbb{Z}/N\mathbb{Z})^*$ מתקיים $e_N(a)\le l<\phi(N)$ ואין ל-N שורש פרימיטיבי. ■

[27] מהטענה הקודמת נובע שאכן קיים a כזה.
[28] בהכרח אחד מהם זוגי והאחר אי-זוגי ושניהם שורשים פרימיטיביים של p^k שהרי הם שקולים מודולו p^k.
[29] קיימת רק שארית אחת מודולו N ששקולה ל-1 בשני המודולוסים הזרים n ו-m והיא 1 מודולו N.

טענה 3.11. אם N מתחלק ב-4 ובראשוני אי-זוגי אז אין ל-N שורשים פרימיטיביים.

הוכחה. נניח ש-N מתחלק ב-4 ובראשוני אי-זוגי ויהיו $k,m\in\mathbb{N}$ כך ש-$N=2^k\cdot m$ ו-$m\in\mathrm{Odd}$, מהנתון נובע ש-$2\le k$, $3\le m$ ו-$\gcd\left(2^k,m\right)=1$.
נסמן $l:=\mathrm{lcm}\left(\phi\left(2^k\right),\phi\left(m\right)\right)$, מהגדרה מתקיים $l\mid\phi\left(2^k\right)$ וגם $l\mid\phi\left(m\right)$ ולכן ממשפט אוילר נובע שלכל $\overline{a}\in\left(\mathbb{Z}/N\mathbb{Z}\right)^*$ מתקיים:

$$a^l\equiv 1\mod 2^k$$
$$a^l\equiv 1\mod m$$

ומכאן שע"פ משפט השאריות הסיני מתקיים גם $a^l\equiv 1\mod N$.
כעת נשים לב לכך ש-$\phi\left(2^k\right),\phi\left(m\right)\in\mathrm{Even}$ ולכן בהכרח $l<\phi\left(2^k\right)\cdot\phi\left(m\right)=\phi\left(N\right)$ ומכאן שלכל $\overline{a}\in\left(\mathbb{Z}/N\mathbb{Z}\right)^*$ מתקיים $e_N\left(a\right)\le l<\phi\left(N\right)$ ואין ל-N שורש פרימיטיבי. ∎

טענה 3.12. אם קיים $2<k\in\mathbb{N}$ כך ש-$N=2^k$ אז אין ל-N שורש פרימיטיבי.

הוכחה. נניח שקיים k כנ"ל ונוכיח את הטענה באינדוקציה על k.
עבור $k=3$ מתקיים $2^k=8$ ול-8 אכן אין שורשים פרימיטיביים:

$$1^1\equiv 1\mod 8\qquad 5^2\equiv 1\mod 8$$
$$3^2\equiv 1\mod 8\qquad 7^2\equiv 1\mod 8$$

כעת נניח באינדוקציה שהטענה נכונה עבור $3\le k\in\mathbb{N}$ כלשהו ונוכיח עבור $k+1$.
נסמן $n:=2^k$, ויהי $a\in\mathbb{Z}$ זר ל-2^{k+1} (כלומר $a\in\mathrm{Odd}$).
מטענה 3.1 נקבל ש-$e_n\left(a\right)\mid\phi\left(n\right)=2^{k-1}$ ומהנחת האינדוקציה נובע ש-$e_n\left(a\right)<\phi\left(n\right)=2^{k-1}$ וממילא מתקיים:

$$a^{\left(2^{k-2}\right)}\equiv 1\mod 2^k$$

א"כ יהי $q\in\mathbb{Z}$ כך ש-$a^{\left(2^{k-2}\right)}=1+2^k\cdot q$.

$$\Rightarrow a^{\left(2^{k-1}\right)}=\left(1+2^k\cdot q\right)^2=1+2\cdot 2^k\cdot q+2^{2k}\cdot q^2\equiv 1\mod 2^{k+1}$$

אבל $2^{k-1}<2^k=\phi\left(2^{k+1}\right)$ ומכאן ש-a אינו שורש פרימיטיבי מודולו 2^{k+1}. ∎

מסקנה 3.13. יש ל-N שורש פרימיטיבי אם"ם קיים $2<p\in\mathbb{N}$ ראשוני כך ש-$N\in\{2,4\}\cup\left\{p^k\mid k\in\mathbb{N}\right\}\cup\left\{2p^k\mid k\in\mathbb{N}\right\}$, כלומר אם"ם N הוא 2, 4, חזקה של ראשוני אי-זוגי או 2 כפול חזקה של ראשוני אי-זוגי.

♣ השערת ארטין: בהינתן $a\in\mathbb{Z}$ שאינו ריבוע, האם קיימים אינסוף ראשוניים ש-a הוא שורש פרימיטיבי שלהם? ההשערה רוצה לומר שכן אך זו עדיין בעיה פתוחה במתמטיקה ולא קיים אפילו $a\in\mathbb{Z}$ אחד שאינו ריבוע שעבורו נפתרה הבעיה.

4 שאריות ריבועיות וחוק ההדדיות הריבועית

טענה 4.1. יהי $2 < p \in \mathbb{N}$ מספר ראשוני, מתקיים:

$$\left|\left\{x^2 : 0 \neq x \in \mathbb{F}_p\right\}\right| = \frac{p-1}{2}$$

כלומר מספר השאריות הריבועיות השונות מ-0 בשדה $\mathbb{Z}/p\mathbb{Z}$ (או מספר השאריות הריבועיות השונות מאפס מודולו p) הוא $\frac{p-1}{2}$.

♣ הריבועים הם כל הריבועים של $\frac{p-1}{2}$ האיברים ה"ראשונים" בשדה מפני שהשאר הם הנגדיים שלהם.

הוכחה. כל מה שצריך להוכיח הוא שלכל $a, b \in \mathbb{Z}$ מתקיים $a \equiv \pm b \mod p \iff a^2 \equiv b^2 \mod p$ וזה קורה מכיוון ש-$a^2 - b^2 \equiv (a+b)(a-b) \mod p$ ו-$\mathbb{Z}/p\mathbb{Z}$ הוא שדה. ■

טענה 4.2. יהיו $2 < p \in \mathbb{N}$ ראשוני $g \in \mathbb{Z}$ שורש פרימיטיבי של p ו-$a \in \mathbb{Z}$ כך ש-$a \not\equiv 0 \mod p$, מהגדרה קיים $n \in \mathbb{N}$ כך ש-$g^n \equiv a \mod p$, יהי n כנ"ל; הפסוקים הבאים שקולים:

- a הוא שארית ריבועית מודולו p.
- n זוגי[30].
- $2e_p(a) \mid p-1$ או אם תרצו $e_p(a) \mid \frac{p-1}{2}$ או $2 \mid \frac{p-1}{e_p(a)}$, בקיצור $\frac{p-1}{2e_p(a)} \in \mathbb{Z}$.

הוכחה. נוכיח תחילה ששני הסעיפים הראשונים שקולים זה לזה:

- $\Leftarrow$

  נניח ש-a הוא שארית ריבועית מודולו p ויהי $s \in \mathbb{Z}$ כך ש-$s^2 \equiv a \mod p$.
  יהי $m \in \mathbb{N}$ כך ש-$g^m \equiv s \mod p$, א"כ מתקיים $g^{2m} \equiv s^2 \equiv a \equiv g^n \mod p$ ולכן מהמשפט הקטן של פרמה נובע ש-$2m \equiv n \mod p-1$ וממילא גם $2m \equiv n \mod 2$ ו-$n \in \text{Even}$.

- $\Rightarrow$

  נניח ש-n זוגי ונסמן $s := g^{\frac{n}{2}} \in \mathbb{Z}$, מכאן שמתקיים $s^2 \equiv g^n \equiv a \mod p$ ו-a הוא שארית ריבועית מודולו p.

כעת נעבור להוכחת השקילות בין שני הסעיפים האחרונים:

- $\Leftarrow$

  נניח ש-n זוגי ויהי $m \in \mathbb{N}$ כך ש-$n = 2m$,

$$\begin{aligned}\Rightarrow a^{\frac{p-1}{2}} &\equiv (g^n)^{\frac{p-1}{2}} \equiv g^{n\cdot\frac{p-1}{2}} \equiv g^{2m\cdot\frac{p-1}{2}} \\ &\equiv g^{m\cdot(p-1)} \equiv \left(g^{p-1}\right)^m \equiv 1^m \equiv 1 \mod p\end{aligned}$$

  ולכן מטענה 3.1 נובע ש-$\frac{p-1}{2} \mid e_p(a)$.

- $\Rightarrow$

  נניח ש-$\frac{p-1}{2} \mid e_p(a)$ ויהי $m \in \mathbb{N}$ כך ש-$\frac{p-1}{2} = m \cdot e_p(a)$.

$$\Rightarrow g^{n\cdot\frac{p-1}{2}} \equiv (g^n)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \equiv a^{m\cdot e_p(a)} \equiv \left(a^{e_p(a)}\right)^m \equiv 1^m \equiv 1 \mod p$$

  מהיות g שורש פרימיטיבי ומטענה 3.2 נובע שמתקיים $n \cdot \frac{p-1}{2} \equiv 0 \mod p-1$, כלומר $p-1 \mid n \cdot \frac{p-1}{2}$ ולכן n מוכרח להיות זוגי.

■

[30] הזוגיות של n מוגדרת היטב מפני ש-$p-1$ זוגי ולכן מהמשפט הקטן של פרמה לכל $m \in \mathbb{Z}$ כך ש-$g^m \equiv a \mod p$ m זוגי.

טענה 4.3. הסמל של לז'נדר הוא פונקציה כפלית, לכל $2 < p \in \mathbb{N}$ ראשוני ולכל $a, b \in \mathbb{Z}$ מתקיים:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

♣ כרגיל מהכפליות נובע שמספיק לבדוק את הסמל על ראשוניים כדי להכיר אותו כראוי.

הוכחה. יהי $2 < p \in \mathbb{N}$ ראשוני, יהיו $a, b \in \mathbb{Z}$. ונניח תחילה ש-a ו-b אינם מתחלקים ב-p.
יהי g שורש פרימיטיבי של p ויהיו $n, m \in \mathbb{N}$ כך ש-$g^n \equiv a \mod p$ ו-$g^m \equiv b \mod p$.

$$\Rightarrow ab \equiv g^{n+m} \mod p$$

נשים לב ש-$n + m \in \text{Even}$ אם"ם $n, m \in \text{Even}$ או ש-$n, m \in \text{Odd}$, מהטענה הקודמת (4.2) נובע ש-g^{n+m} הוא שארית ריבועית מודולו p אם"ם g^n ו-g^m הם שאריות ריבועיות או ששניהם אינם שאריות ריבועיות, כלומר ab הוא שארית ריבועית אם"ם a ו-b הם שאריות ריבועיות או ששניהם אינם שאריות ריבועיות.

$$\Rightarrow \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

אם a ו/או b מתחלקים ב-p אז גם ab מתחלק ב-p ולכן סמל לז'נדר שלו הוא 0 ומהגדרה גם אגף שמאל הוא 0. ■

משפט 4.4. מבחן אוילר
לכל $2 < p \in \mathbb{N}$ ראשוני ולכל $a \in \mathbb{Z}$ מתקיים:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$$

הוכחה. יהי $2 < p \in \mathbb{N}$ ראשוני ו-$a \in \mathbb{Z}$, אם $a \equiv 0 \mod p$ אז הטענה טריוויאלית, א"כ נניח ש-$a \not\equiv 0 \mod p$.
יהי g שורש פרימיטיבי של p ויהי $n \in \mathbb{N}$ כך ש-$g^n \equiv a \mod p$; מטענה 4.2 נובע שאם a שארית ריבועית אז $n \in \text{Even}$ ולכן גם:

$$a^{\frac{p-1}{2}} \equiv (g^n)^{\frac{p-1}{2}} \equiv \left(g^{p-1}\right)^{\frac{n}{2}} \equiv 1^{\frac{n}{2}} \equiv 1 \equiv \left(\frac{a}{p}\right) \mod p$$

ואם a אינו שארית ריבועית אז $n \in \text{Odd}$ ולכן גם[31]:

$$a^{\frac{p-1}{2}} \equiv (g^n)^{\frac{p-1}{2}} \equiv \left(g^{\frac{p-1}{2}}\right)^n \equiv (-1)^n \equiv -1 \equiv \left(\frac{a}{p}\right) \mod p$$

■

מסקנה 4.5. לכל $2 < p \in \mathbb{N}$ ראשוני מתקיים:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

[31] אנחנו יודעים ש-$g^{\frac{p-1}{2}} \not\equiv 1 \mod p$ ושאם נעלה את $g^{\frac{p-1}{2}}$ בריבוע נקבל את 1 מודולו p, בשדה ($\mathbb{Z}/p\mathbb{Z}$ הוא שדה) יש רק שני שורשים ריבועיים של 1 והם ± 1 ומכאן ש-$g^{\frac{p-1}{2}} \equiv -1 \mod p$.

משפט 4.6. הלמה של גאוס

יהיו $2 < p \in \mathbb{N}$ ראשוני ו-$a \in \mathbb{Z}$ זר ל-p ונסמן ב-n את מספר השאריות המינימליות השליליות[32] בקבוצה $\left\{\{i \cdot a\}_p \mid \frac{p-1}{2} \geq i \in \mathbb{N}\right\}$, מתקיים:

$$\left(\frac{a}{p}\right) = (-1)^n$$

הוכחה. נסמן $S := \left\{\{i \cdot a\}_p \mid \frac{p-1}{2} \geq i \in \mathbb{N}\right\}$, ותהיינה $s_1, s_2, \ldots, s_n \in S$ כל השאריות השליליות ב-S ו-$r_1, r_2, \ldots, r_m \in S$ יתר השאריות ב-S.

נשים לב לכך שלכל $\frac{p-1}{2} \geq i, j \in \mathbb{N}$ כך ש-$i \neq j$ מתקיים $i \cdot a \not\equiv -j \cdot a \mod p$: משום שאחרת יתקיים גם $a \cdot (i+j) \equiv 0 \mod p$ ומכיוון ש-a זר ל-p נדע ש-$i + j \equiv 0 \mod p$ בסתירה לכך ש-i ו-j הם טבעיים שונים הקטנים מ-$\frac{p-1}{2}$ ולכן סכומם אינו עולה על $p-1$; א"כ לכל $n \geq i \in \mathbb{N}$ ולכל $m \geq j \in \mathbb{N}$ מתקיים $-s_i \not\equiv r_j \mod p$ ומכאן שע"פ עקרון שובך היונים מתקיים[33]:

$$\left\{i \in \mathbb{N} \mid i \leq \frac{p-1}{2}\right\} = \{-s_1, -s_2, \ldots, -s_n, r_1, r_2, \ldots, r_m\}$$

$$\Rightarrow \frac{p-1}{2}! = \prod_{i=1}^{n}(-s_i) \cdot \prod_{j=1}^{m} r_j = (-1)^n \cdot \prod_{i=1}^{n} s_i \cdot \prod_{j=1}^{m} r_j$$

כעת נזכור שמהגדרה $S = \{s_1, s_2, \ldots, s_n, r_1, r_2, \ldots, r_m\}$ ולכן:

$$\prod_{i=1}^{n} s_i \cdot \prod_{j=1}^{m} r_j \equiv \prod_{i=1}^{\frac{p-1}{2}} (i \cdot a) \equiv \frac{p-1}{2}! \cdot a^{\frac{p-1}{2}} \mod p$$

$$\Rightarrow \frac{p-1}{2}! = (-1)^n \cdot \frac{p-1}{2}! \cdot a^{\frac{p-1}{2}} \mod p$$

העצרת המופיעה בשקילות היא מכפלה של מספרים זרים ל-p ולכן היא שווה למספר זר ל-p וניתן לחלק בה את שני האגפים.

$$\Rightarrow 1 \equiv (-1)^n \cdot a^{\frac{p-1}{2}} \mod p$$

$$\Rightarrow (-1)^n \equiv a^{\frac{p-1}{2}} \mod p$$

וממבחן אוילר נקבל את המבוקש. ■

♣ בתרגילי החזרה למבחן הוכחנו שאם $p \equiv 3 \mod 4$ אז $\frac{p-1}{2}! \equiv \pm 1 \mod p$, הדרך לעשות זאת הייתה להראות שמתקיים $\left(\frac{p-1}{2}!\right)^2 \equiv 1 \mod p$.

מסקנה 4.7. לכל $2 < p \in \mathbb{N}$ ראשוני מתקיים:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv \pm 1 \mod 8 \\ -1 & p \equiv \pm 3 \mod 8 \end{cases} = \begin{cases} 1 & p \equiv 1 \vee p \equiv 7 \mod 8 \\ -1 & p \equiv 3 \vee p \equiv 5 \mod 8 \end{cases}$$

הוכחה. נשים לב לכך שלכל $\frac{p-1}{4} \geq i \in \mathbb{N}$ מתקיים $\{2i\}_p > 0$ ולכל $i \in \mathbb{N}$ כך ש-$\frac{p-1}{4} < i \leq \frac{p-1}{2}$ מתקיים $\{2i\}_p < 0$, א"כ מספר השאריות המינימליות השליליות בקבוצה $\left\{\{2i\}_p \mid \frac{p-1}{2} \geq i \in \mathbb{N}\right\}$ הוא $n := \frac{p-1}{2} - \left\lfloor \frac{p-1}{4} \right\rfloor$ ומכאן שע"פ הלמה של גאוס מתקיים:

$$\left(\frac{2}{p}\right) = (-1)^n$$

[32] נעבוד ע"פ ההגדרה הראשונה של שאריות מינימליות.

[33] מהגדרה לכל $n \geq i \in \mathbb{N}$ מתקיים $0 < -s_i \leq \frac{p-1}{2}$, כמו כן $r_j \not\equiv 0 \mod p$ לכל $m \geq j \in \mathbb{N}$ מפני ש-a זר ל-p.

יהיו $q \in \mathbb{Z}$ ו-$8 > r \in \mathbb{N}_0$ כך ש-$p = 8q + r$[34], נבחין כי:

$$\frac{p-1}{2} = \begin{cases} 4q & r=1 \\ 4q+1 & r=3 \\ 4q+2 & r=5 \\ 4q+3 & r=7 \end{cases} \qquad \left\lfloor \frac{p-1}{4} \right\rfloor = \begin{cases} 2q & r=1 \\ 2q & r=3 \\ 2q+1 & r=5 \\ 2q+1 & r=7 \end{cases}$$

$$\Rightarrow \frac{p-1}{2} - \left\lfloor \frac{p-1}{4} \right\rfloor = \begin{cases} 6q & r=1 \\ 6q+1 & r=3 \\ 6q+3 & r=5 \\ 6q+4 & r=7 \end{cases}$$

$$\Rightarrow \left(\frac{2}{p}\right) = (-1)^n = \begin{cases} 1 & p \equiv 1 \vee p \equiv 7 \mod 8 \\ -1 & p \equiv 3 \vee p \equiv 5 \mod 8 \end{cases}$$

■

למה 4.8. יהי $a \in \mathbb{Z}$ אי-זוגי זר לראשוני $2 < p \in \mathbb{N}$, נסמן:

$$t := \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor$$

מתקיים:

$$\left(\frac{a}{p}\right) = (-1)^t$$

הוכחה. נבחין כי $\left\lfloor \frac{ka}{p} \right\rfloor$ היא המנה של חלוקת ka ב-p עם שארית, מכאן (נשתמש בסימוני הוכחת הלמה של גאוס) שמתקיים:

$$\begin{aligned} \sum_{k=1}^{\frac{p-1}{2}} ka &= \sum_{k=1}^{\frac{p-1}{2}} p \cdot \left\lfloor \frac{ka}{p} \right\rfloor + \sum_{i=1}^{n} (p + s_i) + \sum_{j=1}^{m} r_j \\ &= np + \sum_{k=1}^{\frac{p-1}{2}} p \cdot \left\lfloor \frac{ka}{p} \right\rfloor + \sum_{i=1}^{n} s_i + \sum_{j=1}^{m} r_j \\ &= p \cdot \left(n + \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor \right) + \sum_{i=1}^{n} s_i + \sum_{j=1}^{m} r_j \end{aligned}$$

וגם:

$$\sum_{k=1}^{\frac{p-1}{2}} k = \sum_{i=1}^{n} (-s_i) + \sum_{j=1}^{m} r_j$$

$$\Rightarrow (a-1) \cdot \sum_{k=1}^{\frac{p-1}{2}} k = \sum_{k=1}^{\frac{p-1}{2}} ka - \sum_{k=1}^{\frac{p-1}{2}} k = p \cdot \left(n + \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor \right) + 2 \cdot \sum_{i=1}^{n} s_i$$

[34] מהגדרה $q \in \mathbb{N}$ ו-$r \in \mathrm{Odd}$.

אבל:

$$\sum_{k=1}^{\frac{p-1}{2}} k = \frac{(p-1)\left(\frac{p-1}{2}+1\right)}{4} = \frac{(p-1)\cdot\frac{p+1}{2}}{4} = \frac{p^2-1}{8}$$

$$\Rightarrow (a-1)\cdot\frac{p^2-1}{8} = p\cdot\left(n+\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{ka}{p}\right\rfloor\right)+2\cdot\sum_{i=1}^{n} s_i$$

ומכאן נובע כי (נזכור ש-p ו-a אי-זוגיים):

$$0 \equiv (a-1)\cdot\frac{p^2-1}{8} \equiv p\cdot\left(n+\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{ka}{p}\right\rfloor\right) \equiv n+\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{ka}{p}\right\rfloor \mod 2$$

$$\Rightarrow t = \sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{ka}{p}\right\rfloor \equiv n \mod 2$$
$$\Rightarrow (-1)^t \equiv (-1)^n \mod 2$$

ולכן ע"פ הלמה של גאוס מתקיים:

$$(-1)^t = (-1)^n = \left(\frac{a}{p}\right)$$

■

♣ אם במקום להשתמש בעובדה ש-a אי-זוגי היינו מניחים ש-$a=2$ אז היינו מקבלים שמתקיים:

$$\frac{p^2-1}{8} = (a-1)\cdot\frac{p^2-1}{8} \equiv p\cdot\left(n+\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{ka}{p}\right\rfloor\right) \equiv n+\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{ka}{p}\right\rfloor \mod 2$$

והיות שלכל $\frac{p-1}{2} \geq k \in \mathbb{N}$ מתקיים $\left\lfloor\frac{2k}{p}\right\rfloor = 0$ היה נובע מזה שמתקיים:

$$\frac{p^2-1}{8} \equiv n \mod 2$$

וממילא $(-1)^{\frac{p^2-1}{8}} = (-1)^n$ ולכן גם:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

משפט 4.9. חוק ההדדיות הריבועית

יהיו $2 < p, q \in \text{Prime}$ שונים זה מזה, מתקיים:

$$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

או בעברית פשוטה:

- אם $p \equiv 1 \mod 4$ ו/או $q \equiv 1 \mod 4$ אז p הוא שארית ריבועית מודולו q אם"ם q הוא שארית ריבועית מודולו p (כלומר סימני לז'נדר שלהם זהים).
- אם $p \equiv q \equiv 3 \mod 4$ אז p הוא שארית ריבועית מודולו q אם"ם q אינו שארית ריבועית מודולו p (כלומר סימני לז'נדר שלהם מנוגדים).

♣ חוק ההדדיות הריבועית, הכפליות של סמל לז'נדר והעובדה שמהגדרה סמל לז'נדר עובד לפי המודולוס[35] מאפשרים לנו לבדוק את מספר שלם כלשהו הוא שארית ריבועית במהירות רבה ע"י השלבים הבאים:

1. אם המספר שנמצא בחלק העליון של הסמל גדול מהתחתון אז כותבים אותו מודולו התחתון.
2. אם הוא אינו ראשוני אז מפרקים אותו לראשוניים וכותבים את סמל לז'נדר כמכפלה של כל אחת מהחזקות בנפרד.
3. מחזקות זוגיות ניתן להתעלם ולחזקות אי-זוגיות ניתן להתייחס כהעלקה בחזקת 1.
4. כעת כל המספרים בסמלים הם ראשוניים וניתן להשתמש במשפט ההדדיות הריבועית - אם אחד מהראשוניים שקול ל-1 מודולו 4 ניתן "להפוך" את הסמל ללא שינוי נוסף, אחרת יש להוסיף סימן מינוס בחוץ.
5. חוזרים על ארבעת השלבים הקודמים עבור כל אחד מהסמלים במכפלה, המספרים הולכים וקטנים במהירות עד שניתן לבדוק ישירות את סמלי לז'נדר הנותרים באופן ישיר, בנוסף התהליך הזה ייעצר רק כאשר בחלק העליון של הסמל יופיע הראשוני 2[36] ואז ניתן להשתמש במסקנה 4.7.

הוכחה. נתבונן בשריג[37]:

$$L := \left\{(x, y) \in \mathbb{Z}^2 \mid 0 < x \leq \frac{q-1}{2},\ \ 0 < y \leq \frac{p-1}{2}\right\}$$

מהגדרה מתקיים $|L| = \frac{q-1}{2} \cdot \frac{p-1}{2}$.
נסמן:

$$L_1 := \left\{(x, y) \in L \mid \frac{p}{q} \cdot x \geq y\right\}$$
$$L_2 := \left\{(x, y) \in L \mid \frac{p}{q} \cdot x \leq y\right\}$$

מהגדרה מתקיים $L = L_1 \cup L_2$, אך יתרה מזאת זהו איחוד זר מפני שלו הייתה קיימת נקודה $(x, y) \in L$ כך ש-$\frac{p}{q} \cdot x = y$ היינו מקבלים ש-$q \mid x$ בסתירה לכך ש-$0 < x \leq \frac{q-1}{2}$; א"כ מתקיים $|L| = |L_1| + |L_2|$.
לכל $\frac{p-1}{2} \geq i \in \mathbb{N}$ ולכל $\frac{q-1}{2} \geq j \in \mathbb{N}$ מתקיים:

$$|\{(x, y) \in L_1 \mid y = i\}| = \left\lfloor \frac{i \cdot q}{p} \right\rfloor$$
$$|\{(x, y) \in L_2 \mid x = j\}| = \left\lfloor \frac{j \cdot p}{q} \right\rfloor$$

[35] כלומר אם מספר כלשהו הוא שארית ריבועית אז כל מספר אחר ששקול לו לפי המודולוס גם הוא שארית ריבועית באותו מודולוס.
[36] סמל לז'נדר אינו מוגדר עבורו ולכן א"א "להפוך" את הסמל כשמגיעים אליו.
[37] דמיינו את הקבוצה כאוסף נקודות במישור הנמצאות בהצטלבויות של קווי האורך והרוחב השלמים.

$$\Rightarrow t_2 := |L_2| = \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{i \cdot q}{p} \right\rfloor$$
$$\Rightarrow t_1 := |L_1| = \sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{j \cdot p}{q} \right\rfloor$$

נזכור שע"פ הלמה האחרונה (4.8) מתקיים:

$$\left(\frac{q}{p}\right) = (-1)^{t_2}$$
$$\left(\frac{p}{q}\right) = (-1)^{t_1}$$

$$\Rightarrow \left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{t_2+t_1} = (-1)^{|L_2|+|L_1|}$$
$$= (-1)^{|L|} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

■

טענה 4.10. יהי $2 < p \in \text{Prime}$ ויהי $a \in \mathbb{Z}$ שארית ריבועית שונה מאפס מודולו p, a הוא שארית ריבועית מודולו p^k לכל $k \in \mathbb{N}$.

♣ כדי להוכיח את הטענה נמיר השאלה אם $a \in \mathbb{Z}$ הוא שארית ריבועית מודולו p^k כאשר p ראשוני בשאלה אם יש לפולינום $x^2 - a$ שורש מודולו p ואז נשתמש בלמה של הנזל[38].

♣ ממסקנה 1.15 נובע שאם מספר $a \in \mathbb{Z}$ הוא שארית ריבועית מודולו p ראשוני לכל ראשוני המופיע בפירוק של מספר $1 < N \in \mathbb{N}$ אז הוא גם שארית ריבועית מודולו N.

♣ מה קורה כאשר מדובר במעריך גדול מ-2? בכיתה עסקנו רק במקרים שבהם המעריך הוא ראשוני (בטענה הבאה).

טענה 4.11. יהיו $2 < p, q \in \text{Prime}$ ו-$a \in (\mathbb{Z}/p\mathbb{Z})^*$, נתבונן בקונגרואנציה $x^q \equiv a \mod p$;

- אם $p = q$ אז ע"פ המשפט הקטן של פרמה יש לקונגרואנציה פתרון יחיד והוא a.
- אם $p \not\equiv 1 \mod q$ אז q זר ל-$p-1$ ולכן יש לו הופכי מודולו $p-1$ ומהמשפט הקטן של פרמה נקבל שקיים פתרון יחיד והוא $a^{q^{-1}}$[39].
- אם $p \equiv 1 \mod q$ נסמן ב-g שורש פרימיטיבי של p ויהי $m \in \mathbb{N}$ כך ש-$a \equiv g^m \mod p$, כעת יש לקונגרואנציה פתרון אם"ם $q \mid m$[40] ואז קבוצת הפתרונות היא:

$$\left\{ g^{\frac{m}{q} + k \cdot \frac{p-1}{q}} \mid q > k \in \mathbb{N}_0 \right\}$$

[38] הנגזרת $(2x)$ לעולם לא תתאפס מפני ש-2 זר ל-p^e לכל $e \in \mathbb{N}$ ואם $s^2 \equiv a \mod p^e$ עבור $e \in \mathbb{N}$ כלשהו אז העובדה ש-a זר ל-p^e מחייבת שגם s זר ל-p^e.

[39] כאשר q^{-1} הוא ההופכי של q מודולו $p-1$.

[40] נשים לב שיחס החלוקה הזה מוגדר היטב מפני ש-$q \mid p-1$.