חשבון מודולרי - טענות בלבד

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 $\overline{f(x)} = \bar{0}$.

♣ 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 $\bar{a}, \bar{b} \in (\mathbb{Z}/N\mathbb{Z})^*$ מתקיים $\bar{a} \cdot \bar{b} \in (\mathbb{Z}/N\mathbb{Z})^*$.

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 $a^{p-1} \equiv 1 \mod p$.

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 $a^{\phi(N)} \equiv 1 \mod N$.

♣ 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 $p^{\text{Ord}_p(N)}$ לכל p ראשוני המחלק את N.

♣ 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 וכך אכן נעשה בקובץ ההוכחות.

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

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

$$x \equiv 1 \mod 3$$
$$x \equiv 2 \mod 5$$
$$x \equiv 2 \mod 7$$

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 (בשעון של 5) את 6 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[3]. 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[4], כלומר לכל $n, m \in \mathbb{N}$ הזרים זה לזה מתקיים $\phi(n \cdot m) = \phi(n) \cdot \phi(m)$.

[3] ניתן היה גם להתייחס ל-$2-7$ כ--5 ואז היינו מקבלים $37 \mod 105 \equiv 7 + (-5) \cdot 15 = -68$ (והרי $105 = 3 \cdot 5 \cdot 7$).

[4] בהמשך, כשנלמד על פונקציות אריתמטיות, נקרא לפונקציה אריתמטית כזו כפלית סתם למרות שזו אינה ההגדרה הרגילה של פונקציה כפלית.

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[5], מתקיים:

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

♣ 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-$\phi\left(n\right)=2^k$ אם"ם כל הראשוניים האי-זוגיים בפירוק של n הם ראשוני פרמה והריבוי שלהם הוא 1.

1.3 משפטים נוספים

משפט 1.20. משפט וילסון (Wilson)[6]

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

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

עבור $p=2$ המשפט טריוויאלי, נראה כעת שתי הוכחות עבור $p\neq2$.

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

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 $p\equiv1\mod 4$.

טענה 1.23. קיימים אינסוף ראשוניים השקולים ל-1 מודולו 4, כלומר הקבוצה $\{p\in\mathrm{Prime}\mid p\equiv1\mod 4\}$ היא קבוצה אינסופית.

טענה 1.24. קיימים אינסוף ראשוניים השקולים ל-3 מודולו 4, כלומר הקבוצה $\{p\in\mathrm{Prime}\mid p\equiv3\mod 4\}$ היא קבוצה אינסופית.

♣ 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 $A\cdot x\equiv b\mod N$[7] 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[8] 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.

---

[5] כלומר לכל $r\geq i,j\in\mathbb{N}$ מתקיים $p_i=p_j\iff i=j$.

[6] ערך בוויקיפדיה האנגלית: John Wilson.

[7] הכוונה היא שהווקטורים בשני האגפים מחושבים מעל $\mathbb{Z}$ ומתקיימת שקילות מודולו N בכל קואורדינטה.

[8] אולי ניתן לתקן אותו אך כפי שלמדנו אותו הוא כבר לא עובד משום שהוא השתמש בכפל בהופכי ע"מ לייצר אחדות מובילים.

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[9]

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-$f'(a)\not\equiv 0 \mod p$[10]
אז קיים $b\in\mathbb{Z}$ כך ש-$b\equiv a \mod p^e$ וגם $f(b)\equiv 0 \mod p^{e+1}$[11]; 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 $f'(a)\not\equiv 0 \mod p$.

♣ 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.

[9] ערך בוויקיפדיה: קורט הנזל.
[10] פולינום הנגזרת של פולינום בעל מקדמים שלמים שייך גם הוא לחוג הפולינומים מעל השלמים.
[11] 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.

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. $f * g = g * f$ - הקונבולוציה 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:

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

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 $\sigma_1 = \phi * \sigma_0$.[12]

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

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 $i, j \in \mathbb{N}$[13], 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 $\{a^k \mid k \in \mathbb{N}\} = (\mathbb{Z}/N\mathbb{Z})^*$.

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.

למה 3.5. יהי $n \in \mathbb{N}$, נסמן ב-D את קבוצת המחלקים הטבעיים של n ותהיינה $f, g : D \to \mathbb{C}$[14], אם לכל $d \in D$ מתקיים $\sum_{0<e|d} f(e) = \sum_{0<e|d} g(e)$ אז $f = g$.

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

♣ בפרט, לכל $p \in \mathbb{N}$ ראשוני קיימים $\phi(p-1)$ 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 $a^p \not\equiv b^p \mod p^{t+1}$.

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

טענה 3.9. יהיו $2 < p \in \mathbb{N}$ ראשוני, $k \in \mathbb{N}$ ו-$a \in \mathbb{Z}$ שורש פרימיטיבי של p^k[15], המספר האי-זוגי מבין a ו-$a + p^k$[16] הוא שורש פרימיטיבי של $2p^k$.

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

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

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

מסקנה 3.13. יש ל-N שורש פרימיטיבי אם"ם קיים $2 < p \in \mathbb{N}$ ראשוני כך ש-$N \in \{2,4\} \cup \{p^k \mid k \in \mathbb{N}\} \cup \{2p^k \mid k \in \mathbb{N}\}$, 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.

[13] 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.

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

[15] מהטענה הקודמת נובע שאכן קיים a כזה.

[16] בהכרח אחד מהם זוגי והאחר אי-זוגי ושניהם שורשים פרימיטיביים של p^k שהרי הם שקולים מודולו p^k.

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.

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[17].
- $2e_p(a) \mid p-1$ או אם תרצו $e_p(a) \mid \frac{p-1}{2}$ או $2 \mid \frac{p-1}{e_p(a)}$, בקיצור $\frac{p-1}{2e_p(a)} \in \mathbb{Z}$.

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.

משפט 4.4. מבחן אוילר

לכל $2 < p \in \mathbb{N}$ ראשוני ולכל $a \in \mathbb{Z}$ מתקיים:

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

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

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

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

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[18] בקבוצה $\left\{ \{i \cdot a\}_p \mid \frac{p-1}{2} \geq i \in \mathbb{N} \right\}$, מתקיים:

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

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

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

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

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:

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

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

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

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

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[19] 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[20] ואז ניתן להשתמש במסקנה 4.7.

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[21].

♣ 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 $a^{q^{-1}}$[22].
- 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 $q \mid m$[23] ואז קבוצת הפתרונות היא:

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

[19] כלומר אם מספר כלשהו הוא שארית ריבועית אז כל מספר אחר ששקול לו לפי המודולוס גם הוא שארית ריבועית באותו מודולוס.

[20] סמל לז'נדר אינו מוגדר עבורו ולכן א"א "להפוך" את הסמל כשמגיעים אליו.

[21] 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.

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

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