חשבון מודולרי - הגדרות 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 $1 < N \in \mathbb{N}$.

הגדרה 1.1. נאמר ששני מספרים $x, y \in \mathbb{Z}$ הם קונגרואנטיים/שקולים מודולו N אם $N \mid (x - y)$ ואז נסמן $x \equiv y \mod N$.

♣ כמובן שזהו יחס שקילות.

♣ הרעיון הוא ששאריות החלוקה של x ו-y ב-N שוות.

♣ N הנ"ל נקרא המודולוס.

סימון: לכל $x \in \mathbb{Z}$ נסמן ב-$\overline{x}$ את מחלקת השקילות של x ביחס הנ"ל, כלומר $\overline{x} := \{y \in \mathbb{Z} \mid x \equiv y \mod N\}$, מסמנים את קבוצת מחלקות השקילות ב-$\mathbb{Z}/N\mathbb{Z}$, כאשר אנו עובדים עם יותר ממודולוס אחד נסמן את מחלקות השקילות ע"י $[x]_N$.

♣ למה לסמן $\mathbb{Z}/N\mathbb{Z}$ ולא פשוט $\mathbb{Z}/N$?
הסימון $N\mathbb{Z}$ הוא בעצם האידיאל $N \cdot \mathbb{Z} = \{N \cdot a \mid a \in \mathbb{Z}\}$ והסימון R/I כאשר R הוא חוג ו-I הוא אידיאל בחוג משמש לסימון לחוג המנה המושרה על R ע"י I, חוג המנה הוא קבוצת מנה (כלומר קבוצת מחלקות שקילות) המושרית ע"י הגדרת מחלקת השקילות של איבר a בחוג בצורה הבאה: $[a] := \{a + r \mid r \in I\}$, כלומר מבחינה אינטואיטיבית אנחנו "מאפסים" את כל איברי האידיאל (הם שקולים ל-0) וכל שני איברים בחוג שקולים זה לזה אם ההפרש ביניהם שייך לאידיאל (כלומר שאריות החלוקה שלהם[1] ביוצר של החוג שוות). רעיון דומה מופיע במרחבי מנה שעליהם למדנו בלינארית 1: גם שם לקחנו תמ"ו W של מ"ו V והגדרנו את מחלקת השקילות של וקטור $v \in V$ ע"י $[v] := \{v + w \mid w \in W\}$ וכמו שכאן קבוצת מחלקות השקילות היא חוג שם קבוצת מחלקות השקילות היא מרחב וקטורי.
מה שאני רוצה לומר בהערה הזו הוא שפעמים רבות לסימונים מתמטיים יש משמעות כללית שאינה נובעת מההקשר המסוים שבו אנו עוסקים, כך למשל הסימון $\mathbb{F}[x]$ לחוג הפולינומים מעל שדה הוא בסך הכל דוגמה לסימון $A[x]$ כאשר A היא קבוצה שעליה מוגדרות פעולות חיבור וכפל ו-x הוא משתנה פורמלי המאפשר לנו לדבר על פולינום מהצורה $ax^2 + bx + c$ וכדומה.

הגדרה 1.2. נאמר שקבוצה $\{r_1, r_2, \ldots, r_N\}$ היא מערכת נציגים שלמה אם לכל $N \geq i, j \in \mathbb{N}$ כך ש-$i \neq j$ מתקיים $\overline{r_i} \neq \overline{r_j}$.

למה 1.3. לכל $a, b \in \mathbb{Z}$ ולכל $x \in \overline{a}$ ו-$y \in \overline{b}$ מתקיים $\overline{a \pm b} = \overline{x \pm y}$ וגם $\overline{a \cdot b} = \overline{x \cdot y}$.

הגדרה 1.4. נגדיר פעולות חיבור, חיסור וכפל על $\mathbb{Z}/N\mathbb{Z}$: לכל $\overline{a}, \overline{b} \in \mathbb{Z}/N\mathbb{Z}$ נגדיר את פעולות החיבור והחיסור ע"י $\overline{a} \pm \overline{b} := \overline{a \pm b}$ ואת פעולת הכפל ע"י $\overline{a} \cdot \overline{b} := \overline{a \cdot b}$.

למה 1.5. לכל $x \in \mathbb{Z}$ מתקיים $\overline{x} = \{x + k \cdot N \mid k \in \mathbb{Z}\}$.

♣ לכן קיימות N מחלקות שקילות שנציגיהן הם: $0, 1, 2, \ldots, N - 1$.

למה 1.6. מהשוויון $\overline{x} = \{x + k \cdot N \mid k \in \mathbb{Z}\}$ נובע גם שלכל $a, b \in \mathbb{Z}$, אם $a \equiv b \mod N$ אז $\gcd(a, N) = \gcd(b, N)$.

הגדרה 1.7. לכל $\overline{a} \in \mathbb{Z}/N\mathbb{Z}$ נגדיר את המחלק המשותף המקסימלי של $\overline{a}$ ו-N להיות $\gcd(a, N)$ ונסמן אותו ב-$\gcd(\overline{a}, N)$.

סימון: נסמן $(\mathbb{Z}/N\mathbb{Z})^* := \left\{\overline{a} \mid \exists \overline{b} \in \mathbb{Z}/N\mathbb{Z} : \overline{a} \cdot \overline{b} = 1\right\}$[2].

---

[1] אם ניתן לבצע חילוק עם שארית בחוג.

[2] ה-"*" היא סימון כללי לקבוצת האיברים ההפיכים בחוג מסוים יש המסמנים אותה ע"י "×" במקום "*", אבל כמו שהברווז מוחתם בלידתו גם אני "נדבק" לסימונים הראשונים שאני רואה ולכן אשתמש רק ב-"*".

טענה 1.8. הקבוצה $\mathbb{Z}/N\mathbb{Z}$ היא חוג חילופי, כלומר היא מקיימת את כל אקסיומות השדה (ביחס לפעולות החיבור והכפל שהגדרנו) מלבד קיום הופכי לכל איבר שונה מ-0, כאשר $\overline{0}$ הוא האיבר האדיש לחיבור ו-$\overline{1}$ הוא האיבר האדיש לכפל.

- ♣ כאשר N ראשוני הקבוצה $\mathbb{Z}/N\mathbb{Z}$ היא גם שדה (נהוג לסמנו ב-$\mathbb{F}_N$), ראינו זאת בליניארית 1.
- ♣ כל הטענות שאנחנו מכירים על שדות ואינן משתמשות באקסיומת ההופכי נכונות גם עבור חוג חילופי, כך למשל **אם** יש לאיבר הופכי אז הוא יחיד ולכן יש משמעות לסימון $\overline{a}^{-1}$ (וכמובן גם ל-$-\overline{a}$).

למה 1.9. יהי $\overline{a} \in \mathbb{Z}/N\mathbb{Z}$, $\overline{a} \in (\mathbb{Z}/N\mathbb{Z})^*$ (כלומר $\overline{a}$ הפיך מודולו N) אם"ם $\gcd(a, N) = 1$.

הגדרה 1.10. פונקציית אוילר
תהא $\phi : \mathbb{N} \to \mathbb{N}$ המוגדרת ע"י $\phi(n) := |\{n \geq m \in \mathbb{N} : \gcd(n, m) = 1\}|$[3] לכל $n \in \mathbb{N}$, כלומר ϕ מחזירה את מספר המספרים הקטנים או שווים ל-n[4] שגם זרים ל-n.

- ♣ אם $n \neq 1$ אז $\phi(n) = \left|(\mathbb{Z}/n\mathbb{Z})^*\right|$.
- ♣ לכל $p \in \mathbb{N}$ ראשוני מתקיים $\phi(p) = p - 1$.

מסקנה 1.11. אם N הוא ראשוני אז לכל איבר שונה מאפס יש הופכי ו-$\mathbb{Z}/N\mathbb{Z}$ הוא שדה.

2 פונקציות אריתמטיות

הגדרה 2.1. נסמן $\mathcal{F} := \{f : \mathbb{N} \to A \mid A \subseteq \mathbb{C}\}$ (כלומר קבוצת הסדרות ב-$\mathbb{C}$[5]) ונקרא ל-$\mathcal{F}$ קבוצת הפונקציות האריתמטיות.

- ♣ נתעניין בפונקציות $f \in \mathcal{F}$ המקיימות ש-$f(n)$ תלוי בתכונות אריתמטיות של n (זו כמובן הסיבה לשם של $\mathcal{F}$), קצת קשה להגדיר זאת...

הגדרה 2.2. נאמר על פונקציה אריתמטית f שהיא כפלית אם לכל $n, m \in \mathbb{N}$ הזרים זה לזה מתקיים $f(n \cdot m) = f(n) \cdot f(m)$, נסמן את קבוצת הפונקציות הכפליות ב-$\mathcal{M}$.

- ♣ זה שונה מאד מהמובן הרגיל של כפליות.

הגדרה 2.3. תהיינה $f, g \in \mathcal{F}$, נגדיר את הקונבולוציה $f * g : \mathbb{N} \to \mathbb{C}$ (נקראת גם קונבולוציית דיריכלה) ע"י (לכל $n \in \mathbb{N}$):

$$(f * g)(n) := \sum_{0<d|n} f(d) \cdot g\left(\frac{n}{d}\right)$$

- ♣ למרות שממבט ראשון הגדרת הקונבולוציה אינה סימטרית למעשה היא דווקא כן כזו מפני שאם נסמן $D := \left\{(a, b) \in \mathbb{Z}^2 \mid a \cdot b = n\right\}$ נקבל:

$$(f * g)(n) = \sum_{(a,b)\in D} f(a) \cdot g(b)$$

[3] יש המסמנים את פונקציית אוילר ב-φ אך מכיוון שאודי השתמש ב-ϕ גם אני אעשה זאת כאן (שוב ההחתמה).
[4] הנפקא מינה היחידה של הא"ש החלש היא ש-$\phi(1) = 1$.
[5] ניתן היה להחליף את $\mathbb{C}$ בכל שדה או בכל קבוצה שמוגדרות עליה פעולות חיבור וכפל.

2.1 דוגמאות חשובות

דוגמה 2.4. תהא $\delta:\mathbb{N}\to\{0,1\}$ המוגדרת ע"י (לכל $n\in\mathbb{N}$):

$$\delta\left(n\right):=\begin{cases}1 & n=1\\0 & n\neq1\end{cases}$$

דוגמה 2.5. לכל $k\in\mathbb{N}_0$ נגדיר את הפונקציה $I_k:\mathbb{N}\to\mathbb{N}_0$ ע"י (לכל $n\in\mathbb{N}$):

$$I_k\left(n\right):=n^k$$

♣ כן, זה נראה קצת מגוחך ואולי זה באמת כך, כמובן שעבור $k=0$ נקבל $I_0\equiv1$.

דוגמה 2.6. לכל $k\in\mathbb{N}_0$ נגדיר את $\sigma_k:\mathbb{N}\to\mathbb{N}_0$ ע"י (לכל $n\in\mathbb{N}$):

$$\sigma_k\left(n\right):=\sum_{0<d|n}d^k$$

♣ מהגדרה $\sigma_0\left(n\right)$ הוא מספר המחלקים הטבעיים של n.

♣ מספר משוכלל הוא כזה המקיים $n=\sigma_1\left(n\right)$.

דוגמה 2.7. פונקציית אוילר (הגדרה 1.10).

דוגמה 2.8. תהא $\mu:\mathbb{N}\to\{-1,0,1\}$ <u>פונקציית מביוס</u>[6] המוגדרת ע"י (לכל $n\in\mathbb{N}$):

- אם n אינו חופשי מריבועים אז $\mu\left(n\right):=0$
- אם n חופשי מריבועים אז $\mu\left(n\right):=\left(-1\right)^k$ כאשר k הוא מספר הראשוניים המחלקים את n (שמהגדרה שונים זה מזה)

♣ כלומר אם n חופשי מריבועים אז $\mu\left(n\right)$ הוא -1 אם מספר הראשוניים המחלקים את n אי-זוגי ו-1 אם הוא זוגי (בפרט $\mu\left(1\right)=1$).

דוגמה 2.9. תהא $S:\mathbb{N}\to\mathbb{N}_0$ פונקציה המוגדרת ע"י $S\left(n\right):=\left|\left\{x^2\mid x\in\mathbb{Z}/n\mathbb{Z}\right\}\right|$, כלומר $S\left(n\right)$ הוא מספר השאריות הריבועיות מודולו n (כולל 0).

---

[6] ערך בוויקיפדיה: אוגוסט פרדיננד מביוס.

3 שורשים פרימיטיביים

יהי $1 < N \in \mathbb{N}$.

הגדרה 3.1. לכל $\overline{a} \in (\mathbb{Z}/N\mathbb{Z})^*$ נסמן $e_N(a) := \min\left\{k \in \mathbb{N} \mid a^k \equiv 1 \mod N\right\}$ ונקרא ל-$e_N(a)$ המעריך של a מודולו N (יש הקוראים לו גם האקספוננט או הסדר של a מודולו N).

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

הגדרה 3.2. יהי $\overline{a} \in (\mathbb{Z}/N\mathbb{Z})^*$, נאמר ש-$a$ הוא שורש פרימיטיבי של N אם $e_N(a) = \phi(N)$.

4 שאריות ריבועיות וחוק ההדדיות הריבועית

הגדרה 4.1. נאמר ש-$a \in \mathbb{Z}$ (או $\overline{a} \in \mathbb{Z}/N\mathbb{Z}$) הוא שארית ריבועית מודולו N אם קיים $b \in \mathbb{Z}$ כך ש-$b^2 \equiv a \mod N$.

הגדרה 4.2. סמל לז'נדר[7]

נסמן $P := \text{Prime} \setminus \{2\}$, הסמל של לז'נדר (נקרא גם סימן לז'נדר) הוא הפונקציה $\left(\frac{\cdot}{\cdot}\right) : \mathbb{Z} \times P \to \{1, -1, 0\}$ המוגדרת ע"י (לכל $a \in \mathbb{Z}$ ו-$2 < p \in \text{Prime}$):

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & a \equiv 0 \mod p \\ 1 & a \not\equiv 0 \mod p, \ \exists x \in \mathbb{Z} : x^2 \equiv a \mod p \\ -1 & a \not\equiv 0 \mod p, \ \nexists x \in \mathbb{Z} : x^2 \equiv a \mod p \end{cases}$$

או בעברית: סימן לז'נדר של a הוא 0 אם a הוא 0 מודולו p, 1 אם הוא שארית ריבועית שונה מאפס מודולו p ו--1 אחרת.

טענה 4.3. לכל $2 < p \in \mathbb{N}$ ראשוני ולכל $a, b \in \mathbb{Z}$ מתקיים:

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \Longleftrightarrow a \equiv b \mod p$$

♣ הסמל של לז'נדר הוא דוגמה לקרקטר דיריכלה.

הגדרה 4.4. שארית מינימלית

יהיו $2 < p \in \mathbb{N}$ ראשוני ו-$a \in \mathbb{Z}$, ישנן שתי הגדרות לשארית מינימלית שמאחוריהן עומד אותו רעיון:

1. השארית המינימלית של a מודולו p היא האיבר היחיד בקטע $\left(-\frac{p-1}{2}, \frac{p-1}{2}\right)$ השקול ל-a מודולו p.
2. השארית המינימלית של a מודולו p היא האיבר היחיד בקטע $[0, p)$ השקול ל-a מודולו p.

נסמן את השארית המינימלית של a מודולו ע"י $\{a\}_p$.

[7] ערך בוויקיפדיה: אדריאן-מארי לז'נדר.