עכשיו אנחנו מציגים חומר שבאותו קרוי "תורת המספרים" (מה שעשינו עד כה היה כלי עזר בסיסיים - אינדוקציה ועקרון הסדר הטוב שעזרו לנו בהוכחות).
תורת המספרים הוא תחום מתמטי שעוסק במספרים שלמים, הטבעיים וכו', וכמה שזה נשמע פשוט, יש בו המון השערות פתוחות קשות כמו.
לדוג': - השערת גולדבך - כל זוגי חוץ מ-2 הוא סכום של 2 ראשוניים
(ספר מומלץ: הדוד פטרוס והשערת גולדבך)
- המשפט האחרון של פרמה: אין טבעיים x,y,z המקיימים $x^3+y^3=z^3$ (וכן אם נחליף את 3 ב-4 או יותר, והשם משפט פרמה).

בשולי הספר אריתמטיקה של דיופנטוס

פרמה כתב במאה ה-17 שהוא מצא הוכחה נפלאה אבל שולי הדף קטנים מלהכילה. בשנת 95' אנדרו-וויילס נתן הוכחה. ד' עמודים אינסופיים.
(כ-200 עמודים בערך).
אפשר לקרוא את הספר "המשפט האחרון של פרמה" / סיימון סינג.

משפט החלוקה

אומר שתמיד אפשר לבצע חילוק עם שארית. לדוג':

$17 \div 5 = 3\ (2)$ $\qquad 17 = 5\cdot 3 + 2$ ← השארית תמיד קטנה מ-5

$a \div b = q\ (r)$ $\qquad a = bq + r \qquad r<b$

משפט החלוקה: נניח $a\in\mathbb{Z}$, $b\in\mathbb{N}$, אז קיימים $q,r\in\mathbb{Z}$ יחידים כך ש- $a=bq+r$ וכך ש- $0\le r\le b-1$.

סימון: $3|6$ "3 מחלק את 6" אבל $4\nmid 6$ "4 לא מחלק את 6"
$a|b$ אם יש $c\in\mathbb{Z}$ כך ש- $ca=b$. אחרת $a\nmid b$.

הוכחת משפט החלוקה: קיום (של q,r), יחידות

כאן ההוכחה שונה, שונה בהרצאה ממה שיש בסיכום →

[קיום]: (אין נוכיח קיום? הכלי היחיד שלנו הוא עסה"ט ⟸ אינדוקציה. כאן יותר נוח להשתמש ב-עסה"ט)

נשתמש בגרסה "לכל $S\subseteq\mathbb{N}$ לא ריקה יש איבר מינימלי". (הסדר נכון על $\mathbb{N}$ אבל עובד גם אותו דבר).

נגדיר $S=\{a-bk \mid k\in\mathbb{Z} \text{ וגם } a-bk\geq 0\}$ ("המועמדים להיות r") ובוחרים מביניהם ש-r יהיה המינימלי.

(נראה קיום תנאי עקרון הסדר הטוב): • $S\subseteq\mathbb{N}\cup\{0\}$ בהגדרה.

• $S\neq\emptyset$: עלינו להראות שיש מספר מהצורה $a-bk$ שהוא ≥ 0.

אכן, אם $0\leq a$ אז עבור $k=0$: $\underbrace{a-b\cdot 0}_{\in S}\geq 0$.

ואם $a<0$ אז ניקח $k=a$ ⟸

$a-b\cdot a\in S \Leftarrow a-bk=a-ab=\overset{\text{שלי}}{a}(\underbrace{1-b}_{\leq 0 \text{ כי } b>0})\geq 0$

לכן לפי עקרון הסדר הטוב יש ב-S איבר מינימלי r.

המשך

נניח כי r מתקבל ע״י $k=q$ ולכן $r = a-bq$ (q שלם), $r \geq 0$ מהגדרה S.

(מה עוד חסר בשביל להוכיח קיום?) נותר להראות $r<b$.

נניח בשלילה $b\le r$ ⇐ $b\le a-bq$ ⇐ $0\le \underbrace{a-bq-b}_{a-b(q+1)}$

כי $r=a-bq$

ונקבל סתירה למינימליות של r, כלומר מה שכן קטן מ-r ב-S

זה מספר בהגדרה של $a-bk$ שהוא חיובי וגם יותר קטן מאשר $r=a-bq$ (כי הוא שווה ל- $r-b$ ו- $0<b$)

סתירה למינימליות של r

משל קיום.

יחידות: נניח קיימים q_1,q_2,r_1,r_2 שלמים ו- $0\le r_1,r_2\le b-1$ כך ש

$$\begin{cases} a=bq_1+r_1 \\ a=bq_2+r_2 \end{cases}$$

ונרצה להראות שהכרח $q_1=q_2$ ו- $r_1=r_2$.

אכן

$$bq_1+r_1=bq_2+r_2$$
$$\Downarrow$$
$$b(q_1-q_2)+(r_1-r_2)=0$$
$$\Downarrow$$
$$b(q_1-q_2)=r_2-r_1$$
$$\Downarrow$$
$$b\mid \underbrace{r_2-r_1}$$

("b מחלק את r_2-r_1" כלומר r_2-r_1 כפולה של b)

ניזכר כי $0\le r_1,r_2<b$

(איך ייתכן שהפרש של 2 מס' בין 0 ל-b היה כפולה של b? רק אם הם שווים זה לזה)

פורמלי $-b<\underbrace{r_2-r_1}_{\text{כפולה } b}<b$

⇐ $r_2-r_1=0$ ⇐ $r_1=r_2$ ו-

למשל: אם $0\le r_1,r_2<5$ אז
$-5<0-4\le r_2-r_1\le 4-0<5$

⇐ $b(q_1-q_2)=0$ ⇐ $q_1=q_2$.

משל יחידות

משפט החלוקה - גרסה מורחבת: נניח $a,b\in\mathbb{Z}$ כך ש- $b\neq 0$. אז קיימים $q,r\in\mathbb{Z}$ יחידים כך ש- $a=bq+r$ וכן $0\le r<|b|$.

לדוגמה:

$\cancel{-3\ (2)\ \overline{17}\,)(-5)}$ השארית חייבת להיות חיובית

$\cancel{17=(-5)(-3)+2}$

שארית חיובית

$4\ (3)$
$\overline{-17}\,)(-5)$
$-17=(-5)\cdot 4+3$.

<u>הוכחה</u> (מומלץ לקריאה עצמית)

עבור $b>0$ כבר הוכחנו.

נניח $b<0$ ⇐ $|b| = -b > 0$

נפעיל את משפט החלוקה על $|b|$, a

ונקבל $a = l|b| + r$, $0 \le r < |b|$

שקיימים $l, r \in \mathbb{Z}$ יחידים

⇐ $a = l(-b) + r$ —״—

$a = \underbrace{(-l)}_{q} \cdot b + r$ —״—

לזכור ממתמ׳ שנה

$$|x| = \begin{cases} x & \text{אם } 0 \le x \\ -x & \text{אם } 0 > x \end{cases}$$

למשל

$|5| = 5$

$|-5| = -(-5)$

<u>משל.</u>

<u>דוגמה 2</u> - שתלמד אותנו גם איך לעשות "ניסוי" להוכחות:

מתבוננים במס׳ אי־זוגי בריבוע:

$1^2 = 1$ $\quad (-1)^2 = 1$

$3^2 = 9$ $\quad (-3)^2 = 9$

$5^2 = 25$ $\quad \vdots$

$7^2 = 49$

$9^2 = 81$

מה השארית בחלוקה ב-8? נראה 1

<u>טענה</u>: לכל $m \in \mathbb{Z}$ אי זוגי, m^2 משאיר שארית $\boxed{1}$ בחלוקה ב-8.

<u>ניסיון הוכחה ראשון</u>: $m = 2k+1$ אפשר להציג כך לפי משפט החלוקה עם $b=2$.

$$m^2 = (2k+1)^2 = \underbrace{4k^2 + 4k}_{\substack{\text{זה לכאורה נראה} \\ \text{כפולה של 4 ולא כפולה של 8.}}} + 1$$

יש דרך להתגבר על זה... תחשבו לבד...

(קל יותר שעוד צעד אחד כדי להגיע לפורמולת משפט החלוקה צריך לחלק למקרים לפי איזו שארית m משאיר בחלוקה ב-2 (דוגמה 4.10 בספר של אילנה).

<u>ניסיון הוכחה שני</u>:

מתבוננים על חלוקת המספרים האי״ז לפי השארית שנותנים בחלוקה ב-4

$$\underbrace{\{2k+1 \mid k \in \mathbb{Z}\}}_{\text{כל האי״ז}} = \overbrace{\underbrace{\{4k+1 \mid k \in \mathbb{Z}\}}_{\substack{\text{משאירים 1 בחלוקה} \\ \text{ב-4}}} \cup \underbrace{\{4k+3 \mid k \in \mathbb{Z}\}}_{\substack{\text{משאירים 3} \\ \text{בחלוקה ב-4}}}}^{\text{הצגה לפי משפט החלוקה עם } b=4}$$

אם m מהצורה $m = (4k+1)$ ⇐

$m^2 = (4k+1)^2 =$

$= 16k^2 + 8k + 1 =$

$= 8(2k^2 + k) + 1 =$

$= 8n + 1$

נגיד?

אם m מהצורה $m = 4k+3$

$m^2 = (4k+3)^2 =$

$= 16k^2 + 24k + 9 =$

$= 8(2k^2 + 3k) + 8 + 1 =$

$= 8(2k^2 + 3k + 1) + 1$

$= 8n + 1$

ננסח את מה שהוכחנו בצורה פורמלית כדי ללמוד סימונים:

$$\underset{\text{לכל}}{\forall k\in\mathbb{Z}}\ \underset{\text{קיים}}{\exists n\in\mathbb{Z}}\ \underbrace{\text{such that}}_{\text{כך ש}}\ (4k+1)^2=8n+1$$

"לכל $k\in\mathbb{Z}$ קיים $n\in\mathbb{Z}$ כך ש $(4k+1)^2=8n+1$".

וכן: $\forall k\in\mathbb{Z}\ \exists n\in\mathbb{Z}$ s.t. $(4k+3)^2=8n+1$

[כאן אני מדלגת על פיתוח 4.10 – 4.14 שבם מה שבו לשלב החלופה.]

דוגמה 1: יהי $a\in\mathbb{N}$. הוכיחו כי $3\mid a^3-a$

בדיקות בסיס: $a=1 \Rightarrow 3\mid 0$

$a=2 \Rightarrow 3\mid \underbrace{2^3-2}_{6}$

$a=3 \Rightarrow 3\mid \underbrace{3^3-3}_{24}$

פתרון:

$\boxed{a^3-a=a(a^2-1)=(a-1)a(a+1)}$ לפי משפט החלוקה, אם נחלק את a ב-3 השארית תהיה 0 או 1 או 2. לכן מתקיים בדיוק אחד מהבאים:

- $a=3k$ עבור $k\in\mathbb{Z}$ $\Rightarrow a^3-a=(a-1)\cdot 3k\cdot(a+1)=3[k(a-1)(a+1)]$ מתחלק ב-3
- או $a=3k+1$ " " $\Rightarrow a^3-a=3k\cdot a\cdot(a+1)=3[k\cdot a(a+1)]$ " "
- או $a=3k+2$ " " $\Rightarrow a^3-a=(a-1)\cdot a\cdot(3k+3)=3[(a-1)a(k+1)]$ " "

הערה: ערך תחתון - (אינטואיטיבית: לעגל כלפי מטה) $\lfloor -6.5\rfloor=-7$ $\lfloor \frac{3}{5}\rfloor=0$ $\lfloor 2.7\rfloor=2$

הגדרה: לכל $x\in\mathbb{R}$ $\lfloor x\rfloor$ הוא השלם הגדול ביותר שקטן או שווה x.

שאלה: כמה יש כפולות חיוביות של 3 שקטנות או שוות מ-100? $3\cdot1, 3\cdot2, \dots, 3\cdot33, \cancel{3\cdot34}$ $\lfloor\frac{100}{3}\rfloor$

" " " 7 " " $\lfloor\frac{100}{7}\rfloor$

למה: לכל $\underset{100}{x\in\mathbb{R}}$, $\underset{3}{d\in\mathbb{N}}$: $|\{y\in\mathbb{N} \mid d|y \text{ and } 0<y\le x\}|=\lfloor\frac{x}{d}\rfloor$

גודל הקבוצה | המקיימים | כל כפולות d שגדולות מ-0 וקטנות מ-x

הוכחה: כל כפולות d החיוביות הן מהצורה kd עבור $k\in\mathbb{N}$ והמספרים האפשריים אלה $1,\dots,\lfloor\frac{x}{d}\rfloor$.