רבעון למתמטיקה

ללמוד ולמחקר

בעריכת דב ירדן

כרך 3 | ירושלים, כסלו תש"י, דצמבר 1949 | חוברת 4

תכן

כתבת המערכת: דב ירדן, כנסת החדשה, ירושלים

המחיר 250 פרוטה

הוכחה פשוטה למשפט וולסטנהולם

שלמה זכאי

המשפט של וולסטנהולם אומר: אם p מספר ראשוני, הגדול מ 3, הרי המונה של סכום השברים

$$S=\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\dots+\frac{1}{p-1}$$

מתחלק ל p^2. [1]

ההוכחה: נסדר את איברי הסכום S בצורה הבאה:

$$S=\left(\frac{1}{1}+\frac{1}{p-1}\right)+\left(\frac{1}{2}+\frac{1}{p-2}\right)+\dots+\left(\frac{1}{\frac{p-1}{2}}+\frac{1}{\frac{p+1}{2}}\right)$$

$$=p\cdot\left[\frac{1}{1.(p-1)}+\frac{1}{2.(p-2)}+\dots+\frac{1}{\frac{p-1}{2}.\left(p-\frac{p-1}{2}\right)}\right]$$

את הסכום בתוך הסוגרים המרובעים נסמן ב S' ונקבל $S=p.S'$. עכשיו עוד נוכיח כי גם המונה של S' מתחלק ל p.

נשים לב לעובדה כי במכנים של S' מופיעים כל המספרים מ 1 עד $p-1$, מסודרים בזוגות כך, שסכום שני הערכים בכל זוג שוה p. על כן אפשר לכתב את S' בצורה:

$$S'=\sum_{x=1}^{\frac{p-1}{2}}\frac{1}{x(p-x)}$$

אבל היות ובין שני הגורמים x ו $p-x$ תמיד אחד זוגי והשני בלתי-זוגי, אפשר להוכח בנקל, כי גם הבטוי

$$S''=\sum_{x=1}^{\frac{p-1}{2}}\frac{1}{2x(p-2x)}$$

מכיל בדיוק כל אותם שברים, הכלולים בתוך הסכום S'. ועל כן $S''=S'$.

ניצור עכשיו את ההפרש $4S''-S'$, ונקבל:

$$3S'=4S''-S'=\sum\left(\frac{2}{x(p-2x)}-\frac{1}{x(p-x)}\right)=\sum\frac{p}{x(p-x)(p-2x)},$$

$$3S'=p.\sum\frac{1}{x(p-x)(p-2x)}.$$

מכאן, כי $p|3S'$ ומכאן, כי $p|S'$. והיות ו $S=pS'$, יוצא כי $p^2|S$, מש"ל.

בדרך דומה נוכל להוכיח גם את המשפט הבא:

מוני השברים

$$A=\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\dots+\frac{1}{(p-1)^2},\qquad B=\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\dots+\frac{1}{((p-1)/2)^2}$$

מתחלקים ב p, אם p ראשוני גדול מ 3.

באמת,

---

1) Hardy-Wright, An Introduction to the Theory of Numbers, Theorem 115.

$$A=\left(\frac{1}{1^2}+\frac{1}{(p-1)^2}\right)+\left(\frac{1}{2^2}+\frac{1}{(p-2)^2}\right)+\dots+\left(\frac{1}{(p-1)^2/4}+\frac{1}{(p+1)^2/4}\right)$$

$$=\frac{p^2-2p+2.1^2}{1^2(p-1)^2}+\frac{p^2-4p+2.2^2}{2^2(p-2)^2}+\dots+\frac{p^2-2p((p-1)/2)+2((p-1)/2)^2}{((p-1)/2)^2(p-((p-1)/2))^2}=pk+2B,$$

$$B=\sum_{x=1}^{(p-1)/2}\frac{1}{(p-x)^2}=B_1,\quad B_1=\sum_{x=1}^{(p-1)/2}\frac{1}{(p-2x)^2},$$

$$3B=4B_1-B=\sum\left(\frac{4}{(p-2x)^2}-\frac{1}{(p-x)^2}\right)=\sum\frac{4(p-x)^2-(p-2x)^2}{(p-x)^2(p-2x)^2}=\sum\frac{3p^2-4px}{(p-x)^2(p-2x)^2},$$

$$B=\frac{p}{3}\sum\frac{3p-4x}{(p-x)^2(p-2x)^2}.$$

Simple proof of Wolstenholme's theorem

Shlomo Zakay

(Summary)

Wolstenholme's theorem: "The numerator of

$$S=1+\frac{1}{2}+\frac{1}{3}+\dots+\frac{1}{p-1}$$

is divisible by p^2, if p is a prime >3" is here proved as follows.

$$S=\left(\frac{1}{1}+\frac{1}{p-1}\right)+\left(\frac{1}{2}+\frac{1}{p-2}\right)+\dots+\left(\frac{1}{(p-1)/2}+\frac{1}{(p+1)/2}\right)$$

$$=\frac{p}{1.(p-1)}+\frac{p}{2.(p-2)}+\dots+\frac{p}{\frac{p-1}{2}.(p-\frac{p-1}{2})}=pS'$$

$$S'=\sum_{x=1}^{(p-1)/2}\frac{1}{x(p-x)}=S'',\quad S''=\sum_{x=1}^{(p-1)/2}\frac{1}{2x(p-2x)},$$

$$3S'=4S''-S'=\sum\left(\frac{2}{x(p-2x)}-\frac{1}{x(p-x)}\right)=\sum\frac{p}{x(p-x)(p-2x)},$$

$$S'=\frac{p}{3}\sum\frac{1}{x(p-x)(p-2x)}.$$

Similarly the following theorem is proved.

The numerators of

$$A=\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\dots+\frac{1}{(p-1)^2},\qquad B=\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\dots+\frac{1}{((p-1)/2)^2}$$

are divisible by p, if p is a prime >3.

על מכפלות של מספרים שלמים

נתן אליוסף (קבקר)

פרק ראשון.

1. נתון מספר טבעי m. נסמן ע"י $Z=Z(m)$ את קבוצת $\varphi(m)$ המספרים הטבעיים הקטנים מ- m וזרים לו. קבוצה A החלקית ל Z תקרא בשם אגוד $\bmod m$ (בקצור: אגוד) אם יחד עם a היא תכיל גם את $1/a$. ($1/a$ הוא הפתרון היחיד שיש לקונגרואנציה $ax\equiv 1 \bmod m$ המקים את התנאי $1\leq x\leq m-1$ והשייך אפוא ל Z.)

דוגמות: א) $\{1\}$. ב) $\{1,m-1\}$. ג) Z.

2. נמצא את מספר האגודים המכילים רק אבר אחד. נסמן את מספרם ב- $N=N(m)$. ברור כי N הוא מספר הפתרונות מתוך Z של הקונגרואנציה:

$$t^2\equiv 1 \bmod m \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

3. משפט-עזר א'. הפתרונות היחידים של $t^2\equiv 1 \bmod p^a$ (p מספר ראשוני איזוגי) מתוך $Z(p^a)$ הם p^a-1, 1.

הוכחה: p^a צריך לחלק את t^2-1, כלומר את $(t-1)(t+1)$. המחלק המשותף המקס' בין שני הגורמים האלה מחלק את $(t+1)-(t-1)=2$, ועל כן הוא 1 או 2. מאחר ש p^a הוא איזוגי יוצא כי הוא מחלק את אחד הגורמים, ועל כן $t\equiv\pm 1 \bmod p^a$.

משפט-עזר ב'. אם $a>2$, הפתרונות היחידים של $t^2\equiv 1 \bmod 2^a$ מתוך $Z(2^a)$ הם ארבעה המספרים 2^a-1, $2^{a-1}\pm 1$, 1.

הוכחה: ה- t, במקרה זה, צריך להיות איזוגי. נניח כי $t=2c+1$, ולכן $(2c+1)^2\equiv 1 \bmod 2^a$ או $c(c+1)\equiv 0 \bmod 2^{a-2}$ (כאן $a-2>0$). המספרים c, $c+1$ זרים ביניהם ולכן אחד מהם מתחלק ע"י 2^{a-2}. בצורה זאת מקבלים את 4 הפתרונות הדרושים.

משפט-עזר ג'. הפתרונות של $t^2\equiv 1 \bmod 4$ הם $\{1,3\}$. הפתרון של $t^2\equiv 1 \bmod 2$ הוא $\{1\}$.

ההוכחה מידית.

4. נניח כי $2^a\prod p_i^{a_i}$ היא ההצגה הקנונית של m. מאחר שהפונקציה $N(m)$ היא כפלית, על כן $N(m)=N(2^a)\prod N(p_i^{a_i})$. נסמן את מספר ה p_i (האיזוגיים) ע"י s. נקבל:

משפט 1. א) אם $m\equiv 0 \bmod 8$, יהיה $N(m)=2^{s+2}$.
ב) אם m מתחלק ב 4 אבל לא ב- 8, יהיה $N(m)=2^{s+1}$.
ג) אם m איננו מתחלק ב 4, יהיה $N(m)=2^s$.

5. כמקרה פרטי מהסעיף הקודם נקבל:

משפט 2. $N(m)$ מתחלק ב- 4, פרט למקרה ש- m הוא באחת הצורות הבאות: 2, 4, p^a, $2p^a$. במקרים אלה (פרט ל- $m=2$) יהיה $N(m)=2$.

נוח יהיה להשתמש במונח הבא: מספר טבעי m שהוא באחת הצורות 4, p^a, $2p^a$ יקרא בשם מספר סינגולרי.

נוכל לנסח את המשפט האחרון כך: אם $m\neq 2$, תמיד $N(m)$ מתחלק ב- 4 אם m אינו סינגולרי. במקרה ש- m סינגולרי $N(m)=2$.

6. נסמן ב- $P(A)$ את מכפלת כל אברי האגוד A. מאחר שביחד עם a מופיע גם $1/a$, הרי מכפלת שני אברים אלה תתן $a.(1/a)\equiv 1 \mod m$ בתנאי ש- $a\neq 1/a$. על כן ישארו ב- $P(A)$ רק אותם הגורמים הפותרים את הקונגרואנציה (1). נכתב איפוא:

$$P(A)\equiv\prod a_i \mod m$$

כאשר $a_i^2\equiv 1 \mod m$.

נסמן $A'=\{a_1,a_2,\dots\}$. הקבוצה A' היא גם כן אגוד mod m. הוא יקרא בשם __האגוד המצומצם של A__ וההצגה $P(A)$ בעזרת A' תקרא בשם __ההצגה המצומצמת של $P(A)$__.

מתוך ההצגה המצומצמת נובע, למשל, כי

$$[P(A)]^2\equiv 1 \mod m.$$

__הערה__: אם A' היא הקבוצה הריקה:

$$P(A)\equiv 1 \mod m$$

7. נקרא לאגוד mod m בשם __אגודה mod m__ (בקצור: אגודה) אם ביחד עם a הוא מכיל נוסף ל- $1/a$ גם את $m-a$ (אם $m\neq 2$ ברור כי $a\neq m-a$).

__דוגמות__: א) $\{1,m-1\}$. ב) Z.

8. נחזור אל $P(A)$, ונטפל בהצגה המצומצמת. אם A __אגודה__, אז גם $m-a\in A'$ מאחר ש- $m-a\in A$ וביחד עם a גם $m-a$ פותר את (1). אולם $a.(m-a)\equiv -a^2\equiv -1 \mod m$. לכן:

__משפט 3__. אם A אגודה, קים

$$P(A)\equiv(-1)^{M(A)/2} \mod m.$$

כאן $M(A)$ מסמן את מספר האברים בתוך A הפותרים את (1).

__פרק שני.__

נשתמש במשפטים על אגודים ואגודות כלליים כדי לחקור את התכונות של אגודים ואגודות מיוחדים.

9. בתור דוגמה ראשונה, נעיין בקבוצה Z. קבוצה זאת היא אגודה וקים $N(m)=M(Z)$. על סמך §8 נקבל בעזרת §5:

__משפט 4__ (משפט Wilson המכלל) $P(Z)\equiv 1 \mod m.$, פרט למקרה ש- m הוא סינגולרי. במקרה זה $P(Z)\equiv -1 \mod m$.

__הערה 1__; אם $m=p$ מקבלים את משפט Wilson הרגיל.

__הערה 2__: בספר
Hardy-Wright: An Introduction to the Theory of Numbers, 1938
מופיע המשפט והוכחתו על סמך משפט Bauer (ראה שם).

10. נסמן על ידי $R=R(m)$ את קבוצת השאריות הרבועיות mod m (מתוך $Z(m)$) ועל ידי $Q=Q(m)$ את הקבוצה $Z-R$. הסימנים R',Q' מגדרים על ידי §6. ברור כי הקבוצות R,Q הן אגודים. הקבוצה R היא אגודה רק אם -1 היא שארית רבועית mod m.

11. נסמן על ידי p מספר ראשוני איזוגי המקיים $p=1 \bmod 4$ ועל ידי π מספר ראשוני איזוגי המקיים $\pi=3 \bmod 4$. נוכל בקלות למצוא את R',Q' בשביל ערכים מיוחדים של m על פי משפטי-העזר ב- §3.

<u>משפט-עזר א".</u>

$R'(p^a)=\{1,p^a-1\}$	$R'(\pi^a)=\{1\}$
$Q'(p^a)=$ריקה	$Q'(\pi^a)=\{\pi^a-1\}$

ההוכחה מידית על סמך משפט-עזר א'.

<u>משפט-עזר ב".</u> אם $a\geq 4$: $Q'(2^a)=\{2^{a-1}-1,2^a-1\}$, $R'(2^a)=\{1,2^{a-1}+1\}$.

הוכחה: אם $m=2^a$ $(a\geq 4)$, הפתרונות של (1) הם $\pm 1,2^{a-1}\pm 1$ (משפט-עזר ב'). המספרים $-1,2^{a-1}-1$ אינם שאריות רבועיות, כי אילו היה $x^2=-1,2^{a-1}-1$ $(\bmod 2^a)$ היה נובע $(a\geq 4)$ $x^2=-1 \bmod 4$, מה שלא יתכן. המספר $2^{a-1}+1$ הוא שארית רבועית כאשר $a\geq 4$, ואמנם $(2^{a-2}+1)^2=(2^{a-1}+1) \bmod 2^a$.

<u>משפט-עזר ג".</u>

$R'(2)=\{1\}$	$R'(4)=\{1\}$	$R'(8)=\{1\}$
$Q'(2)=$ריקה	$Q'(4)=\{3\}$	$Q'(8)=\{3,5,7\}$

ההוכחה מידית.

12. נניח כי m מתחלק על ידי לפחות מספר ראשוני אחד p $(p=1 \bmod 4)$. נחשב את Q'. אם $q\in Q'$ הרי $q^2=1 \bmod m$ ולכן $q^2=1 \bmod p$, מה שלא יתכן על סמך משפט-עזר א". על כן Q' היא קבוצה ריקה. לכן:

<u>משפט 5</u>. אם m מתחלק על ידי p $(p=1 \bmod 4)$, יהיה $P(Q)=1 \bmod m$.

אם נשתמש ב- §9, נקבל:

<u>משפט 6</u>. אם m מהצורה $p^a,2p^a$ $(p=1 \bmod 4)$ הרי $P(R)=-1 \bmod m$. אם m איננו סינגולרי ומתחלק על ידי p $(p=1 \bmod 4)$ הרי $P(R)=1 \bmod m$.

13. נשאר לטפל במקרה שההצגה הקנונית של m היא $2^a\prod\pi_i^{a_i}$. נחלק את הדיון לשני מקרים:

(א) $0\leq a\leq 3$. נחשב את R'. אם $r\in R'$ אז $r^2=1 \bmod m$ ועל כן $r^2=1 \bmod \pi_i^{a_i}$ וגם $r^2=1 \bmod 2^a$. על סמך משפטי-עזר א", ג" נובע כי $r=1 \bmod \pi_i^{a_i}$ וגם $r=1 \bmod 2^a$. כידוע, למערכת קונגרואנציות זו יש רק פתרון אחד מודולו מכפלת המודולים, כלומר mod m, ולכן $r=1 \bmod m$. מכאן $R'=\{1\}$. לכן:

<u>משפט 7</u>. במקרה הנדון $P(R)=1 \bmod m$.

אם נשתמש ב- §9, נקבל:

<u>משפט 8</u>. אם m איננו סינגולרי אבל מהסוג הנדון, $P(Q)=1 \bmod m$. אחרת $P(Q)=-1 \bmod m$.

(ב) $a\geq 4$. נסמן $m=2^a\prod\pi_i^{a_i}=2^a m'$. נמצא את R'. אם $r\in R'$ הרי $r^2=1 \bmod m$ ולכן $r^2=1 \bmod m'$. מזה נובע (כמו בדיון ב- (א)) כי $r=1 \bmod m'$. מצד שני, גם $r^2=1 \bmod 2^a$. לזה יש שני פתרונות על פי משפט-עזר ב" והם: $r_1=1 \bmod 2^a$, $r_2=(2^{a-1}+) \bmod 2^a$. במקרה הראשון יתקבל $r=1 \bmod m$ ומהמקרה השני $r=(2^{a-1}m'+1) \bmod m$. ולכן $R'=\{1,\frac{1}{2}m+1\}$. מכאן:

משפט 9. במקרה הנדון $P(R)=(\frac{1}{2}m+1) \bmod m$.

אם נשתמש ב- §9, נקבל (בהביאנו בחשבון כי $(\frac{1}{2}m+1)^2=1 \bmod m$ כי $4\not| a$ ($a\geq 4$)

משפט 10. במקרה הנדון $P(Q)=(\frac{1}{2}m+1) \bmod m$.

פרק שלישי.

בעזרת התוצאות הקודמות נוכל לקבל כמה מסקנות מעניינות.

14. יהי $t_o\in Z$. אם t_o שארית רבועית $\bmod m$, יש מספר x מתוך Z אשר בשבילו $x^2=t_o \bmod m$. נעלה את שני אגפי הקונגרואנציה הזאת בחזקת $\varphi(m)/2$ ונקבל על סמך משפט Euler-Fermat:

$$t_o^{\varphi(m)/2}=1 \bmod m.\ldots\ldots\ldots\ldots(2)$$

נניח, מעתה, כי t_o אינה שארית רבועית. לכל $t\in Z$ יש $t'\in Z$ יחיד המקים את הקשר: $tt'=t_o \bmod m$. תמיד $t\neq t_o$, כי אין t_o שארית רבועית. נכפול זה בזה את כל $\varphi(m)/2$ הקונגרואנציות האלה ונקבל: $P(Z)=t_o^{\varphi(m)/2} \bmod m$.

על סמך §9 נקבל שוב את (2), פרט למקרה ש- m סינגולרי. במקרה הסינגולרי: $t_o^{\varphi(m)/2}=-1 \bmod m$.

אם m הוא p^a או $2p^a$ יהיה (בשני המקרים) $\varphi(m)=p^{a-1}(p-1)$, ולכן בשני המקרים:

$$t_o^{p^{a-1}(p-1)/2}=-1 \bmod p^a.\ldots\ldots\ldots(3)$$

נוכיח כי t_o אינה שארית רבועית $\bmod p$. ואמנם, אחרת, היינו מקבלים על סמך (2) כי $t_o^{(p-1)/2}=1 \bmod p$ ולכן $t_o^{p^{a-1}(p-1)/2}=1 \bmod p^a$. על ידי השואה אל (3) נובע $2=0 \bmod p^a$, בנגוד להנחה (p אי־זוגי). גם ההפך נכון, כלומר, אם t_o אינה שארית רבועית $\bmod p$, היא אינה שארית רבועית $\bmod p^a$ או $\bmod 2p^a$. בסך הכל נקבל:

משפט 11. $t^{\varphi(m)/2}=1 \bmod m$ ($t\in Z$), פרט למקרה שמתקיימים בבת־אחת שני התנאים הבאים: א) m סינגולרי. ב) $(\frac{t}{p})=-1$ (סמל Legendre) כאשר m מהצורה $2p^a$, p^a או $t=3$ כאשר $m=4$. במקרה זה יהיה $t^{\varphi(m)/2}=-1 \bmod m$.

הערה: הקשי בהוכחת המשפט הזה במקרה ש- $m\neq p$ בזה שיש מחלקי אפס $\bmod m$.

15. נסמן את מספר השאריות הרבועיות $\bmod m$ על ידי $e=e(m)$, את $R=R(m)=\{r_1,r_2,\ldots,r_e\}$ ואת הפתרונות של (1) על ידי $t_1,t_2,\ldots,t_N$ (למשל $t_1=1;\ t_N=m-1$).

לכל $r_i\in R$ יש x_i הפותר את הקונגרואנציה:

$$x^2=r_i \bmod m.\ldots\ldots\ldots\ldots(4)$$

ביחד עם x_i גם x_it_j ($j=1,\ldots,N$) פותר את (4) וברור כי אלה הם כל הפתרונות של (4). אם נתן ל- i לעבור על המספרים $1,2,\ldots,e$ ונקבל את המטריצה:

$$\begin{pmatrix} x_1t_1 & x_1t_2 & \ldots & x_1t_N \\ \ldots & \ldots & \ldots & \ldots \\ x_et_1 & x_et_2 & & x_et_N \end{pmatrix}$$

כל המספרים במטריצה זו שונים ביניהם. כל מספר שייך ל- Z וברור כי כל אבר של Z נמצא במטריצה זו. יש לנו אפוא שני בטויים למספר האברים

במטריצה. ועל כן $N\cdot e=\varphi(m)$, מכאן:

<u>משפט 12</u>. מספר השאריות הרבועיות mod m הוא $\varphi(m)/N(m)$ כאשר $N(m)$ נתן על ידי §4.

16. אם $m\neq 2$ יש לקונגרואנציה (1) לפחות 2 הפתרונות $1, m-1$. מכאן נובע כי $N(m)\geq 2$ ולכן $e(m)\leq \varphi(m)/2$.

<u>משפט 13</u>. אם $m\neq 2$ מספר אי-השאריות הרבועיות הוא לפחות כמספר השאריות הרבועיות.

17. נמצא מתי מספר השאריות הרבועיות הוא כמספר אי-השאריות הרבועיות. לשם כך הכרחי ומספיק כי $N(m)=2$. על סמך §5 זה יקרה כאשר m סינגולרי.

<u>משפט 14</u>. מספר השאריות הרבועיות הוא כמספר אי-השאריות הרבועיות אז ורק אז אם m הוא סינגולרי.

On products of integers

Nathan Eljoseph (Kabaker)

(Summary)

Chapter 1 deals with subsets of $Z(m)$ (the set of the $\varphi(m)$ numbers less than m and coprime to m) of two kinds: 1) those which contain together with a number A the number 1/A (1/A belonging to $Z(m)$ and satisfying the congruence $Ax\equiv 1 \bmod m$) 2) the sets of the first kind containing together with A the number m-A.

Using the results of Chapter 1 the generalized Wilson Theorem is obtained and also the following two theorems:

1) The product of the quadratic residues mod m is $\equiv 1 \bmod m$ unless m is in one of the following forms: a) p^a or $2p^a$ where $p\equiv 1 \bmod 4$. b) $2^a\prod p_i^{a_i}$ where $a\geq 4$ and each p_i is $\equiv 3 \bmod 4$. In the first case the product is $\equiv -1 \bmod m$, and in the second $\equiv(\frac{1}{2}m+1) \bmod m$.

2) The product of the quadratic non-residues mod m is $\equiv 1 \bmod m$ unless m is in one of the following forms: a) 4, p^a, $2p^a$ where $p\equiv 3 \bmod 4$. b) as b) above. In the first case the product is $\equiv -1 \bmod m$ and in the second $\equiv(\frac{1}{2}m+1) \bmod m$.

Chapter 3 proves the following two theorems with the help of the results of the previous chapters:

1) If $t\in Z(m)$ then $t^{\varphi(m)/2}\equiv 1 \bmod m$ unless <u>both</u> t is a non-residue mod m and m is of the form 4, p^a, $2p^a$. In the latter case $t^{\varphi(m)/2}\equiv -1 \bmod m$.

2) The number of residues is $\varphi(m)/N(m)$ where $N(m)=2^{s+2}$ if $m\equiv 0 \bmod 8$, $N(m)=2^{s+1}$ if $m\equiv 0 \bmod 4$ but $m\not\equiv 0 \bmod 8$, and $N(m)=2^s$ otherwise. Here s is the number of the different odd primes dividing m.

As a result it is found that the number of the non-residues is greater than the number of the residues, unless a) $m=2$, b) $m=4$, p^a, $2p^a$. In the first case there are no non-residues, and in the second the number of non-residues is equal to the number of residues.

מערכת אכסיומות חדשה לבסיס תורת המספרים הטבעיים

ברוך גרמנסקי

א. תהא A קבוצה שקימת בתוכה רלציה דו-מקומית R. יש לקרוא yRx: „y עוקב את x". אנו קוראים כנהוג ל y העוקב של x ול x הקודם הבלתי אמצעי של y. A ו R מקימים את מערכת האכסיומות דלקמן („מערכת האכסיומות א."):

1. A היא קבוצה בלתי-ריקה.

2. לכל אבר x של A יש עוקב y אחד ויחיד השונה מ x, כלומר מ yRx ו zRx נובע $x \neq y = z$.

3. תהא M קבוצה חלקית איזו שהיא של A שיש לה התכונה שיחד עם כל אבר x של A שהיא מכילה אותו היא מכילה גם את כל האברים y של A העוקבים את x, כלומר מקימים את התנאי yRx („התכונה (M)"). אנחנו מגדירים את הקבוצה M' בתור אותה קבוצה חלקית של M המכילה את כל אותם האברים y של M שהם עוקבים לאיזה אבר x שהוא של M, כלומר מקימים את התנאי: yRx, $x \in M$, $y \in M$. אזי, אם M היא קבוצה בלתי-ריקה, היא מכילה בדיוק אבר אחד שאינו מוכל בתוך M'.

ב. במקום שלוש האכסיומות הנזכרות אפשר להשתמש גם בשלוש האכסיומות הבאות שבהן יש ל A ו R אותה הוראה כמו קודם:

1. הקבוצה A היא אינסופית.

2. ישנו אבר מסוים בתוך A שאנו קוראים לו „1", באופן שאם $x \neq 1$, אזי יש ל x קודם בלתי-אמצעי אחד ויחיד השונה מ x, כלומר מ xRu ו xRv נובע $x \neq u = v$.

3. תהא M קבוצה חלקית איזו שהיא של A שיש לה התכונה שיחד עם כל אבר x של A שהיא מכילה אותו היא מכילה גם כל אבר y של A העוקב את x, כלומר מקים את התנאי yRx. אנחנו מגדירים את הקבוצה M' בתור אותה קבוצה חלקית של M המכילה את כל אותם האברים y של M שהם עוקבים לאבר x איזה שהוא של M, כלומר מקימים את התנאי: yRx, $x \in M$, $y \in M$. אזי, אם M היא קבוצה בלתי-ריקה היא מכילה בדיוק אבר אחד שאינו מוכל בתוך M'.

ג. אנחנו נוכיח עכשיו שמערכת האכסיומות א. היא אכביבלנטית למערכת האכסיומות של פאנו בשביל המספרים הטבעיים. נסמן את הקבוצה היסודית של מערכת האכסיומות של פאנו ב B ואת הרלציה היסודית הקימת בתוך B ב S. אנחנו נוכיח אפוא ש A ו R מקימים את מערכת האכסיומות של פאנו וש B ו S מקימים את מערכת האכסיומות א. את הוכחת האכביבלנציה המקבילה בשביל מערכת האכסיומות המובאת בסעיף ב. נניח להזדמנות אחרת.

נשתמש במערכת האכסיומות של פאנו בצורה שנתן לה א. לנדאו[1] (בשנויים קלים):

1. הקבוצה B היא בלתי-ריקה.

2. לכל אבר x של B קים אבר אחד ויחיד של B המקים את התנאי ySx, כלומר מ ySx ו zSx נובע $x \neq y = z$.

3. ישנו אבר מסוים בתוך B, שאנו קוראים לו „1" והמקים את התנאי של $1Sx$ אין פתרון בתוך B,

4. מ xSu ו xSv נובע $u = v$.

5. תהא N קבוצה חלקית של B המקימת את התנאים a) $1 \in N$ ו b) אם $x \in N$ ו ySx אזי גם $y \in N$. אז $N = B$.

ד. נוכיח קודם שממערכת האכסיומות א. נובעת מערכת האכסיומות של פאנו, כלומר נוכיח ש A ו R מקימים את מערכת האכסיומות האחרונה. האכסיומות 1. ו 2. של פאנו מזדהות עם האכסיומות 1. ו 2. של מערכת האכסיומות א. נגדיר עכשיו את האבר 1 של A בתור אותו אבר יחיד של A שאינו מוכל בתוך A'. (פרוש הדבר הזה הוא שאנחנו לוקחים בתור הקבוצה M של האכסיומה 3. של מערכת האכסיומות א. את הקבוצה A כולה לאחר שהיא באופן מובן מאליו בעלת התכונה (M) ויוצרים את הקבוצה $M' = A'$ המתאימה

---

1) E. Landau, Grundlagen der Analysis, Leipzig 1930, p. 2.

לקבוצה זאת.) אבר כזה צריך להיות קים לאחר שהקבוצה A היא לפי האכסיומה 1. של מערכת האכסיומות א. קבוצה בלתי-ריקה. אנחנו טוענים עכשיו שלתנאי $1Rx$ אין פתרון בתוך A. כי לו היה קים פתרון x בתוך A לתנאי $1Rx$, כי אז היה 1 עוקב של אבר מסוים של A ואז היה צריך להיות מוכל בתוך A' בנגוד להגדרתו. על ידי כך הראינו ש A ו R מקימים את האכסיומה 3. של פ א נ ו.

ה. נוכיח עכשיו בדרך השלילה שהקבוצה A והיחס R מקימים את האכסיומה 4. של פ א נ ו. נניח לשם כך שיש שני קודמים בלתי-אמצעיים שונים u ו v לאבר y של A: yRu ו yRv, $y \in A$, $u \in A$, $v \in A$, $u \neq v$. ניצור את הקבוצה החלקית ה מ י נ י מ ל י ת של A המכילה את האברים u ו v של A ושיש לה התכונה (M),§ נקרא לקבוצת שתוף זו הקבוצה Q. נקח בתור הקבוצה M של האכסיומה 3. של מערכת האכסיומות א. את הקבוצה Q ונסתכל באבר היחיד של Q שאינו מוכל בתוך Q'. נוכח בזה שאבר זה יכול להיות רק האבר u או האבר v של Q. כי לו היה זה אבר אחר של Q כי אז לא היתה Q הקבוצה החלקית ה מ י נ י מ ל י ת של A המקימת את שתי התכונות הנזכרות לעיל. באמת יכולנו אז להשמיט אבר זה מ Q מבלי שהקבוצה המתקבלת על ידי כך לא תהיה בעלת שתי התכונות הנדונות של Q. זה נובע מתוך העובדה שהאבר הנדון בזה אינו שוה לפי ההנחה לא ל u ולא ל v ואיננו עוקב לשום אבר אחר של Q. נוכח עכשיו בכך שאבר זה אינו יכול להיות גם u או v ונבוא כך לידי סתירה עם האכסיומה 3. של מערכת האכסיומות א. נניח למשל שהוא שוה ל u, כלומר ש u הוא האבר היחידי של Q שאין לו קודם בלתי-אמצעי. מכאן נובע שלכל אבר אחר של Q יש קודם בלתי-אמצעי. נסתכל עכשיו בקבוצה החלקית $M=Q'=Q-\{u\}$ שיש לה התכונה (M). נוכיח ש $M'=M$. כי בתור אבר של הקבוצה $Q-\{u\}$ שאין לו קודם בלתי-אמצעי בא בחשבון רק עוקב של u, האבר שהשמטנו אותו מ Q, היות ולכל האברים האחרים של Q' יש קודם בתוך Q ולכן גם בתוך Q'. אבל לפי האכסיומה 2. של מערכת האכסיומות א. האבר היחידי של A העוקב את u הוא y, ול y יש קודם בלתי-אמצעי בתוך Q', והוא v. לכן הגענו לידי סתירה עם האכסיומה 3. של מערכת האכסיומות א.& והוכח אפוא שבתור אבר של Q שאינו מוכל בתוך Q' אינו בא בחשבון לא אבר של Q השונה מ u ו v ולא האבר u של Q. באותו אופן נוכל להוכיח שגם האבר v של Q אינו בא בחשבון בתור אבר כזה. לכן הגענו שוב לידי סתירה עם האכסיומה 3. של מערכת האכסיומות א. והוכח של y אין שני קודמים בלתי-אמצעיים בתוך A, כלומר ש A ו R מקימים אף את האכסיומה 4. של פ א נ ו.

ו. נוכיח עכשיו ש A ו R מקימים אף את אכסיומת האינדוקציה השלמה של פאנו. כידוע אכסיומה זו היא אכביבלנטית למשפט שהקבוצה B היא קשורה לגבי S, כלומר שאי-אפשר לפרק את הקבוצה B לשתי קבוצות חלקיות בלתי-ריקות C ו D באופן ש $C \neq O$, $D \neq O$, $C+D=B$, $CD=O$ ובאופן שלא יהיו קימים שני אברים c ו d בתוך B שיקימו את התנאים $c \in C$, $d \in D$ ו dSc או cSd. לכן די להוכיח שהקבוצה A היא קשורה לגבי R. נוכיח גם דבר זה בדרך השלילה. נניח לשם כך שקימות שתי קבוצות חלקיות בלתי-ריקות C ו D של A המקימות את התנאים $C \neq O$, $D \neq O$, $C+D=A$, $CD=O$ ושאין שני אברים c ו d בתוך A המקימים את התנאים: $c \in C$, $d \in D$ ו dRc או cRd. נסתכל בקבוצה החלקית $M=C$ של A. היא מקימת את התנאי (M). לכן יש בה אבר אחד ויחיד שאינו מוכל בתוך C'. כמו-כן יש אבר אחד ויחיד בתוך D שאינו מוכל בתוך D'. נסתכל עכשיו בקבוצה $A=C+D$. לפי האמור מכיל A ש נ י אברים שאינם מוכלים בתוך $A'=C'+D'$. כי אחרת היתה הקבוצה A קשורה לגבי היחס R. לכן הגענו לידי סתירה עם האכסיומה 3. של מערכת האכסיומות א. והוכח שהקבוצה A היא קשורה לגבי היחס R וש A ו R מקימים אפוא את אכסיומת האינדוקציה השלמה.

ז. נוכיח עכשיו שמערכת האכסיומות א. נובעת ממערכת האכסיומות של פ א נ ו, כלומר ש B ו S מקימים את מערכת האכסיומות א. לשם כך די להוכיח ש B ו S מקימים את האכסיומה 3. של מערכת האכסיומות א. נוכיח גם את זה בדרך השלילה. נניח לשם כך שישנה קבוצה חלקית N בתוך B המקימת את התנאי שיחד עם כל אבר x של B שהיא מכילה אותו היא מכילה גם את האבר y של B המקים את התנאי ySx, ושיש לה לכל הפחות שני אברי-התחלה, כלומר שני אברים a ו n שאינם מוכלים בתוך הקבוצה N' המוגדרת על ידי כך שהיא מכילה רק אותם האברים של N שהם עוקבים לאיזה אבר שהוא של N. מאכסיומת האינדוקציה השלמה נובע שלא רק B, כי אם גם N היא קבוצה קשורה. לכן אפשר למצוא בתוך N שרשרת של אברים $b,c,\ldots,e,f,\ldots,m$ שונים ביניהם ושונים מ a ו n, באופן שבסדרה $a,b,c,\ldots,e,f,\ldots,m,n$ כל שני אברים סמוכים e ו f יהיו קשורים על ידי הרלציה S, כלומר יהיה קים fSe או eSf. אבל מזה ש a ו n הם אברי-התחלה בתוך N נובע: bSa ו mSn. לכן צריך להמצא בסדרה זאת אבר ראשון e, בין האברים d ו f, באופן ש $e \neq a$ ו $e \neq n$ ושקים eSd ו eSf, וזה סותר את האכסיומה 4. של פאנו. הסתירה הזאת מראה ש B ו S מקימים את האכסיומה 3. של מערכת האכסיומות א. והוכחת האכביבלנציה של מערכת האכסיומות א. עם מערכת האכסיומות של פאנו היא שלמה.

§, & במקומות המסומנים בסימנים אלה נשמטו בטעות 2 משפטים. ראה בעמוד הבא.

ח. נ ב נ ה עכשיו את סדרת המספרים הטבעיים מתוך מערכת האכסיומות א. את המספר 1 קבלנו כבר לעיל על ידי כך שלקחנו בתור הקבוצה M של מערכת האכסיומות א. את הקבוצה A כולה ובנינו את האבר היחידי של A שאינו כלול ב A'. באותו אופן נוכל לבנות את המספר 2 על ידי כך שנקח את האבר היחידי של A' שאינו כלול ב $(A')'$, את המספר 3 על ידי כך שנקח את האבר היחידי של $(A')'$ שאינו כלול ב $((A')')'$ וכו'. על ידי כך קבלנו סדרה ...,1,2,3 שקל להוכיח שהיא אינסופית, בעלת אברים שונים וממצה את הקבוצה A, שהאבר 2 הוא העוקב של האבר 1, האבר 3 הוא העוקב של האבר 2 וכו'.

---

§ כלומר ניצור את קבוצת השתוף של כל אותן הקבוצות החלקיות של A המכילות את האברים u ו v של A ושיש להן התכונה (M).

& והוכח ש $Q'=(Q')'$. אבל זוהי בעצמה תוצאה שסותרת את האכסיומה 3. של מערכת האכסיומות א.

A new set of axioms

sufficient for the development of the theory of natural numbers

(Summary)

Baruch Germansky

Let A be a set of elements possessing a relationship R. A and R satisfy the following axioms.

1. A is not empty.

2. To every element x of A there exists a s i n g l e element y different from x standing to it in the relation R: from $x \in A$ there follows $y \in A$, yRx, $y \neq x$ and from zRx there follows $z=y$.

3. Be M any non-empty subset of A having the property that with every element x of A which it contains, it also contains all the elements y of A which satisfy the condition yRx. We define M' as that subset of M which contains all those elements y of M which satisfy the condition: yRx, $x \in M$, $y \in M$. Then there exists e x a c t l y one element in M which is not contained in M'.

There follows a proof of the equivalence of this set of axioms with the set of axioms of P e a n o .

הערה למשפט שרפינסקי על בדידות מספרים ראשוניים

דב ירדן

במאמר בשם Remarque sur la répartition des nombres premiers (Colloquium Mathematicum 1 (1948), 193-194) הוכיח פרופסור Wacław Sierpiński משפט מעניין על תפוצת המספרים הראשוניים. נתן כאן את המשפט וההוכחה בהרצאתו של שרפינסקי בתרגום לעברית.

"ידוע יפה, כי בסדרת כל המספרים הטבעיים ישנם רווחים ארוכים כרצוננו, שאינם מכילים שום מספר ראשוני. באמת, שום מספר מ $n-1$ המספרים העוקבים

$$n!+2, \quad n!+3, \quad \ldots, \quad n!+n$$

אינו ראשוני לשום מספר טבעי $n>1$.

ברצוני להוכיח בזה את התכונה הבאה על תפוצת המספרים הראשוניים:

ישנם מספרים ראשוניים מבודדים מפני הצדדים ברווחים ארוכים כרצוננו.

ביתר דיוק, ברצוני לקבע את ה

מ ש פ ט. לכל מספר טבעי n קים מספר ראשוני $p>n$ כזה שכל אחד מן המספרים $p\pm j$ באשר $j=1,2,\ldots,n$ אינו ראשוני.

ה ו כ ח ה. אם נתון n טבעי, קים -כידוע- מספר ראשוני $q>n+1$. המספר

$$a=\prod_{j=1}^{q-2}(q^2-j^2) \tag{1}$$

הוא בעליל טבעי. הואיל והמספר $(q-2)!$ זר למספר הראשוני q, מסיקים בלי קשי מ (1) כי המספרים a ו q זרים ביניהם.

לפי המשפט של לז'ן-דירכלה על סדרה חשבונית, קים מספר ראשוני

$$p>q \tag{2}$$

מצורת $ak+q$, באשר k הוא מספר שלם. הנוסחה $p=ak+q$ נותנת

$$p\pm j=ak+q\pm j. \tag{3}$$

ב $j=1,2,\ldots,n$ יהיה $j<q-1$. המספר $q\pm j$ הוא לפי (1) מחלק של המספר a וקים $q\pm j>1$; לכן, $q\pm j$ הוא לפי (3) גם כן מחלק של המספר $p\pm j$ וקים $q\pm j<p\pm j$ בגלל (2). ובכן המספר $p\pm j$, באשר $j=1,2,\ldots,n$, אינו ראשוני, מה שהיה להוכיח.

ק ו ר ו ל ר. קימים אין-סוף מספרים ראשוניים שאינם שיכים לשום זוג של מספרים ראשוניים תאומיים.

ואכן, הללו הם כל המספרים הראשוניים p שעבורם המספרים $p\pm 1$ ו $p\pm 2$ אינם ראשוניים[1].

ה ע ר ו ת. הואיל והוכחת המשפט, שנסוחו פשוט מאד, משתמשת במשפט על הסדרה החשבונית, יהיה אולי משום ענין למצוא לו הוכחה אלמנטרית. אין אני יודע אפילו שום הוכחה אלמנטרית של הקורולר[2]."

"1) למשל: כל המספרים הראשוניים מצורת $15k+7$ באשר $k=1,2,\ldots$.

2) להוכחה על-ידי שיטות התורה האנליטית של המספרים ושהנה בכל אפן קלה מאד, ראה למשל את פרסומו של
E. Ullrich, Zum Zwillingssatz von Viggo Brun, Bericht über die Mathematiker-Tagung in Tübingen 23-27, September 1946, p. 139-143."

עד כאן דברי שרפינסקי (בנוסחה (1) מופיע במאמר המקורי בטעות $\sum$ במקום $\prod$).

נוסיף עוד מה שכותב פרופסור שרפינסקי בספרו הפולני Teorja liczb (1925), p. 47 על הוכחת משפט דירכלה על הסדרה החשבונית, וזה לשונו (בתרגום):

"הוכחת המשפט הנ"ל של L e j e u n e - D i r i c h l e t היא אחת מן ההוכחות הקשות של תורת המספרים ואינה נתנת להעברה באמצעים אלמנטריים."

אם R. D. James, הסוקר את מאמרו של שרפינסקי ב Mathematical Reviews 10 (1949), 431, כותב:

"Now that there are elementary proofs of the Dirichlet theorem his proof is technically elementary"

אין אפוא, כפי הנראה, להבין כי נמצאה בינתים הוכחה אלמנטרית למשפט דירכלה, אלא הבדל דיאלקטי יש כאן ועניין של הגדרה מה נקרא "אלמנטרי" ומה לא.

נתן עכשו למשפט ולהוכחה של שרפינסקי הצגה שונה כלשהי, שתוביל אותנו, לפחות במקרה של הקורולר, למקרה פרטי של משפט דירכלה, שיש לו באמת הוכחה אלמנטרית.

מ ש פ ט . קימים מספרים ראשוניים מבודדים משני הצדדים ברוחים ארוכים כרצוננו: לכל מספר ראשוני אי-זוגי q קים מספר ראשוני p כך שכל אחד מן המספרים $p\pm j$ באשר $j=1,2,\ldots,q-2$ הוא מספר פריק.

ה ו כ ח ה . נסמן ב a את מכפלת כל המספרים הראשוניים הקטנים מ $2q-2$ והשונים מ q. מובן כי $(a,q)=1$. לכן קים לפי משפט דירכלה מספר טבעי x כך ש $p=ax+q$ הוא מספר ראשוני. אז $p\pm j=ax+q\pm j$ בשביל $j=1,2,\ldots,q-2$ הם מספרים פריקים, לפי שתמיד יש ל $q\pm j$ מחלק משותף גדול מ 1 עם a, ומחלק זה קטן מ $ax+q\pm j$ לפי ש $q\pm j>0$.

נניח עתה, לשם הוכחת הקורולר של שרפינסקי, $q=5$. אז $2q-2=2.5-2=8$ ו $a=2.3.7=42$. במקרה זה מובילה אפוא אותנו הוכחתנו לסדרה החשבונית $42x+5$. לפי L. E. Dickson, History of the theory of numbers V.1, 419 הוכיח A. S. Bang, Nyt Tidsskrift for Math., 1891, 2B, p. 73-82 באפן אלמנטרי מציאות שין-סוף מספרים ראשוניים בסדרה חשבונית בעלת ההבדל 42. במיוחד יש אין-סוף מספרים ראשוניים בסדרה $42x+5$, מה שמוכיח את הקורולר של שרפינסקי באפן אלמנטרי.

Remark to Sierpinski's theorem on isolated primes

Dov Jarden

(Summary)

Sierpinski's theorem on the distribution of primes, Colloquium Mathematicum 1 (1948), 193-4, is here reproduced in a slightly modfied manner which, by a result of Bang, permits to obtain in an elementary way the following corollary:
There is an infinitude of primes not belonging to any pair of prime pairs.

תקונים לכרכים 1-3

כרך 1

ע' 83

$2^{66}=7378...$ (לפי N. G. W. H. Beeger, Amsterdam במכתבו לעורך מ31 באוקטובר 1949. הנ"ל השוה את "לוח 256 החזקות הראשונות של 2" עד $n=145$ עם לוח בכתב-יד עד מקום זה שברשותו ומצאו נכון פרט לטעות-הדפוס הנ"ל).

ע' 88

ש' 12 מלמטה

מ (7_1 יצא

ש' 8 מלמטה

הרי יהיה לנו בהתחשב עם (7_2 במקום 8) $(x_1a_0,x_0a_1)+x_1a_0+x_0a_1=0$

ש' 3 מלמטה

יתקים x_0a_1 באופן

ע' 89

ש' 9 מלמטה

כלומר לאותו חוג של

ע' 90

ש' 6 מלמטה

כלומר במקום המכפלה a_1y_0

כרך 3

ע' 16

ש' 3

$x_4=x_3^2-2c^4$

תכן כרך 3

קונגרס בינלאומי של מתמטיקאים, 19

Contents of Volume 3

International Congress of Mathematicians, 19

RIVEON LEMATEMATIKA

A QUARTERLY JOURNAL

INTENDED TO PROMOTE MATHEMATICAL RESEARCH
AMONG STUDENTS OF MATHEMATICS

DOV JARDEN, EDITOR

Volume 3 Jerusalem, December 1949 Number 4

CONTENTS

Editor's address: Dov Jarden, Kneset Hachadasha, Jerusalem, Israel