בעיות אחדות בתורת המספרים*

פאול ארדש

רשימה זו דנה בבעיות אחדות בלתי קשורות ביניהן.

1) שתי סדרות אין-סופיות של מספרים שלמים $a_1<a_2<\dots$ ו $b_1<b_2<\dots$ נקראות על-ידי הרשמן [1] מתרחקות (זו מזו) אם לכל A מספר הפתרונות של $|a_i-b_j|<A$ הוא סופי. שרפינסקי [2] בנה c (c מסמן את עצמת הרצף) סדרות של מספרים שלמים שכל שתים מהן מתרחקות, למשל כל שתים מן הסדרות

$$S_\alpha=\{2^n+[n^\alpha]\},\ n=1,2,\dots\ (0<\alpha \text{ ממשי})$$

מתרחקות. הרשמן [1] הוכיח שקימים $\aleph_1$ מספרים ממשיים a_α, $1\le\alpha<\Omega_1$, כך שכל שתים מן הסדרות $[a_\alpha^n]$, $n=1,2,\dots$ מתרחקות. נבנה, בלי שמוש באכסיומת הבחירה, קבוצה מעצמת c של מספרים ממשיים $\{a_t\}$, כך שכל שתים מהסדרות $[a_t^n]$ מתרחקות.

הרשמן [1] העיר שאם הסדרות $[a^n]$ ו $[b^n]$, $n=1,2,\dots$, **אינן** מתרחקות, יש ל-

$$\left|\frac{\log a}{\log b}-\frac{p}{q}\right|<1/b^p \tag{1}$$

אין-סוף פתרונות במספרים שלמים p ו q. (ואכן ברור ש (1) נכון, כי אם ל $|a^q-b^p|<A$ יש ב A מסוים אין-סוף פתרונות, נקבל על-ידי לוגרתמיזציה כי ל $|q\log a-p\log b|<2A/b^p$ יש אין-סוף פתרונות, ו (1) נובע אפוא על-ידי חלוק ב $q\log b$).

נבנה עתה קבוצה של מספרים חיוביים x_t, $\frac{9}{10}<t<1$, כך שאף אחד מן המספרים x_{t_1}/x_{t_2} לא ימלא את (1). אם נשים $a_t=e^{x_t}$ תהיינה אפוא כל שתים מן הסדרות $[a_{t_1}^n]$ ו $[b_{t_1}^n]$ מתרחקות, מה שמשלים את הוכחת משפטנו.

מספר ממשי α נקרא מספר-ליוביל אם אי-השויון

$$\left|\alpha-\frac{p}{q}\right|<1/q^m \tag{2}$$

פתיר לכל $m>0$ במספרים שלמים p ו q. מתוך ההגדרה נובע בברור של-(2) יש באמת אין-סוף פתרונות במספרים שלמים p ו q.

נבנה קבוצה מעצמת c של מספרים ממשיים חיוביים $\{x_t\}$, $\frac{9}{10}<t<1$, כך שאף אחד מן המספרים x_{t_1}/x_{t_2}, $9/10<t_1\ne t_2<1$, לא יהיה מספר-ליוביל, ובכן על אחת כמה וכמה שאף אחד מהם לא ימלא את (1), ומשפטנו יהא מוכח.

נגדיר $u_n=2^{3^n}$. יהי

$$x_t=\sum_{n=1}^{\infty}1/2^{[u_n t]},\quad 9/10<t<1.$$

תחלה נזדקק למשפט-העזר הבא:

* נתקבל יח בניסן תשטו (10.4.55).

משפט-עזר. יהי α מספר ממשי. נניח שקימת סדרה אין-סופית של מספרים שלמים $b_1<b_2<\dots$ הממלאים, בשביל מספר שלם מסוים a_n,

$$b_{n+1}<b_n^{c_1}, \quad |\alpha - \frac{a_n}{b_n}|<1/2b_n^2, \quad (a_n,b_n)=1 \qquad (3)$$

($c_1,c_2,\dots$ מסמנים קבועים מחלטים). אזי אין α מספר-ליוביל.

משפט-עזר זה הוא כמובן ידוע, ולא נוכיחנו אלא לשם השלֵמות. יהי q, $q>b_1$, מספר שלם. בשביל n מסוים מוכרח להיות $b_{n-1}<q\leq b_n$. ובכן לפי (3)

$$|\alpha - \frac{p}{q}| \geqslant |\frac{p}{q} - \frac{a_n}{b_n}| - |\frac{a_n}{b_n} - \alpha| > \frac{1}{qb_n} - \frac{1}{2b_n^2} \geqslant \frac{1}{2qb_n} > \frac{1}{2q^{1+c_1}},$$

או בשביל $m>1+c_1$ יש ל (3) רק מספר סופי של פתרונות, ומכאן כי α איננו מספר-ליוביל, מה שהיה להוכיח.

יהי עתה $\frac{9}{10}<t_1<t_2<1$. נוכיח ש x_{t_2}/x_{t_1} איננו מספר-ליוביל. נתבונן ב-

$$\sum_{k=1}^{n}(1/2^{[u_kt_2]})/\sum_{k=1}^{n}(1/2^{[u_kt_1]})=\frac{e_n}{f_n}(1/2^{[u_nt_2]-[u_nt_1]})=\frac{a_n'}{b_n'}, \qquad (a_n',b_n')=1.$$

באשר e_n ו f_n הם מספרים אי-זוגיים ו $(e_n,f_n)=1$. ברור כי $f_n<2.2^{[u_nt_1]}$ ובכן

$$2^{u_n(t_2-t_1)-1} \leq 2^{[u_nt_2]-[u_nt_1]} \leq b_n' < 2.2^{[u_nt_2]} < 2^{u_n+1} \qquad (4)$$

על-ידי חשבון פשוט בשביל $n>n_o$ נקבל אפוא

$$|x_{t_2}/x_{t_1} - a_n'/b_n'| \leq c_2/2^{u_{n+1}t_1} < 1/2b_n'^2 \qquad (5)$$

(הואיל ולפי (4): $2b_n'^2<8.2^{2u_n}<2^{u_{n+1}\cdot\frac{9}{10}}<2^{u_{n+1}t_1}$).

נסדר עתה את b_n' בהתאם לגודל ונקבל סדרה $b_1<b_2<\dots$. קל לראות שבשביל $n>n_o$

$$c_1 > q/(t_2-t_1)^2 \longrightarrow b_{n+1} < b_n^{c_1} \qquad (6)$$

לשם הוכחת (6) יהי m גדול. נגדיר $2^{u_k+1} \leq m<2^{u_{k+1}+1}$. ובכן

$$2^{u_k} \geqslant \tfrac{1}{2}m^{1/3}. \qquad (7)$$

מ (7) ו (4) נובע אפוא שקים b, למשל $b_r=b_k'$, הממלא

$$m > b_r \geqslant \tfrac{1}{2}2^{u_k(t_2-t_1)} \geqslant \tfrac{1}{4}m^{(t_2-t_1)/3} \qquad (8)$$

נגדיר $2^{u_{l-1}(t_2-t_1)-1}<m\leq 2^{u_l(t_2-t_1)-1}$. ובכן $2^{u_l(t_2-t_1)-1}<4m^3$, או

$$2^{u_l}<(2m)^{3/(t_2-t_1)}. \qquad (9)$$

מ (9) ו (4) נובע אפוא שקים b, למשל $b_s=b_l'$, הממלא

$$m\leq b_s < 2.(2m)^{3/(t_2-t_1)}. \qquad (10)$$

מ (8) ו (10) נובע אפוא כי $s\geq r+1$ ו $b_s<b_r^{c_1}$ לכל $c_1>q/(t_2-t_1)^2$ ו m גדול למדי, מה שמשלים את הוכחת (6).

בעזרת משפט-העזר נובע מ (5) ו (6) כי x_{t_2}/x_{t_1} איננו מספר-ליוביל וברור כי אותו דבר נכון בשביל x_{t_1}/x_{t_2} (שכן אם α הוא מספר-ליוביל, גם $1/\alpha$ הוא מספר-ליוביל), והוכחתנו הושלמה.

יהיה מעניין להוכיח קיום שדה של מספרים ממשיים מעצמת c שאינו מכיל שום מספרי-ליוביל אירציונליים. לא הצלחתי אפילו להוכיח קיום חוג של מספרים ממשיים מעצמת c שאינו מכיל שום מספרי-ליוביל אירציונליים.

2) כמה בעיות בתורת-המספרים האדיטיבית הובילו אותי לבעיה הבאה: יהיו $a_1,a_2,\dots,a_{2n}$ מספרים שלמים שונים הממלאים $1\leq a_i\leq 4n$ ויסמנו $b_1,b_2,\dots,b_{2n}$ את המספרים השלמים הנותרים מתוך הָרֶוח $(1,4n)$. האם נכון שקים תמיד מספר שלם t כך שמספר הפתרונות של $a_i+t=b_j$ גדול מ n או שוה ל n. לא הצלחתי להכריע בבעיה זו. בשימנו $a_i=n+i$, $1\leq i\leq 2n$, נראה מיד שאם מסקנה זו נכונה, היא טובה ביותר.

קל לראות שקים תמיד t כך שמספר הפתרונות של $a_i+t=b_j$ הוא $\geq n/2$. כדי לראות זאת נשים אל לב כי מספר הפתרונות של $a_i+x=b_j$, $-4n<x<4n$, הוא $4n^2$ ובכן בשביל t מתאים קימים בעליל $n/2$ b-ים בסדרה a_i+t. שֶׁרְק [3] הוכיח שבשביל t מתאים, מספר הפתרונות של $a_i+t=b_j$ הוא $\geq(2-\sqrt{2})n$.

3) נסמן ב $A(n)$ את מספר המספרים השלמים $1\leq m\leq n^2$ הנתנים להכתב כמכפלת שני מספרים שלמים שאינם עולים על n. נוכיח ש

$$\lim_{n\to\infty} A(n)/n^2=0$$

באמת, נוכיח שבשביל $\alpha>0$ מסוים

$$A(n)=o(n^2/(\log n)^\alpha) \qquad (11)$$

נסמן ב $f(k)$ את מספר הגורמים הראשוניים של k, כשגורמים כפולים נחשבים לפי כפילותם. מסקנה ידועה של הרדי ורמנוין [4] טוענת שכמעט בשביל כל k, $f(k)=(1+o(1))\log\log k$. ביתר דיוק, לכל ε קים α כך שמספר המספרים השלמים $k\leq n$ שבשבילם $f(k)<(1-\varepsilon)\log\log k$ או $f(k)>(1+\varepsilon)\log\log k$ הוא $o(n/(\log n)^\alpha)$.

נחלק עתה את המספרים השלמים מצורת

$$a.b, \qquad 1\leq a,b\leq n$$

לשתי מחלקות. למחלקה הראשונה שיכים המספרים השלמים שבשבילם קימים כאחת שני אי-השויונות $f(a)>\frac{2}{3}\log\log n$ ו $f(b)>\frac{2}{3}\log\log n$. ברור כי $f(a.b)>\frac{4}{3}\log\log n>(\frac{4}{3}-n)\log\log(n^2)$. מכאן לפי מסקנת הרדי ורמנוין, מספר המספרים השלמים במחלקה הראשונה הוא $o(n^2/(\log n)^\alpha)$. בשביל המספרים השלמים במחלקה השניה נוכל להניח כי $f(a)\leq\frac{2}{3}\log\log n$. אולם אז שוב לפי מסקנת הרדי ורמנוין, מספר הבחירות האפשריות בשביל a הוא $o(n/(\log n)^\alpha$.

ובכן מספר המספרים השלמים במחלקה השניה הוא גם כן $o(n/(\log n)^{\alpha})$, מה שמשלים את הוכחת (11).

נראה כי קשה לתת נוסחה אסמפטוטית בשביל $A(n)$, או אפילו לקבע את החסם העליון הקטן ביותר של ה α-ים שבשבילם קים (11).

בעיה אחרת שונה במקצת שאינני יכול לפתר אותה היא הבאה: תהיינה $1 \le a_1 < a_2 < \dots < a_x \le n$; $1 \le b_1 < b_2 < \dots < b_y \le n$ שתי סדרות של מספרים שלמים שבשבילן המכפלות $a_i \cdot b_j$ כולן שונות. האם נכון הוא ש $xy < c_3 n^2/\log n$? אם מסקנה זו נכונה, היא בלי ספק טובה ביותר, הואיל ואפשר לבחר את ה a-ים כמספרים השלמים $\le \frac{n}{2}$ ואת ה b-ים כמספרים הראשוניים p, $n/2 < p < n$. שיטה אחרת היא לבחר את ה a-ים כמספרים השלמים שכל גורמיהם הראשוניים הם $\equiv 1 \pmod 4$ ואת ה b-ים כמספרים השלמים שכל גורמיהם הראשוניים הם $\equiv 3 \pmod 4$.

האוניברסיטה העברית בירושלים

SOME REMARKS ON NUMBER THEORY (Summary)

Paul Erdös

1) Hartman defines that two sequences $a_1 < a_2 < \dots$ and $b_1 < b_2 < \dots$ are far apart if for any A there are only a finite number of solutions of $|a_i - b_j| < A$. He proves that there exists a set of real numbers $\{a_\alpha\}$, $\alpha < \Omega_1$ of power $\aleph_1$ so that any two of the sequences $[a_\alpha{}^n]$, n=1,2,... are far apart.

We show without using the axiom of choice that there exists a set $\{a_t\}$ of real numbers of power c so that any two of the sequences $[a_t{}^n]$, n=1,2,... are far apart. In connection with the proof the following question arises: Does there exist a field of real numbers of power c no element of which is a Liouville number? I could not decide this question.

2) Let $1 \le a_1 < a_2 < \dots < a_{2n} \le 4n$ be 2n arbitrary integers. $b_1, b_2, \dots b_{2n}$ are the other 2n integers of the interval (1,4n). I show that there exists an integer x so that there are at least n/2 b's among the integers $a_i + x$. Scherk improved this to $(2-\sqrt{2})n$. It is not known whether this can further be improved to n.

3) I prove that the number of integers not exceeding n^2 which can be written as the product of two integers not exceeding n is $o(n^2)$. I also state the following conjecture: Let $a_1 < a_2 < \dots < a_x \le n$; $b_1 < b_2 < \dots < b_y \le n$ be two sequences of integers for which all the products $a_i b_j$ are different. Is it then true that

$$x \cdot y < c \frac{n^2}{\log n}?$$

Hebrew University of Jerusalem