

סמינר בתורת המספרים

הנושא העליון הוא אנליזה דיפרנציאלית. זה מתחלק לשניים:

- משואה דיפרנציאלית

- קירובים דיפרנציאליים

משואה דיפרנציאלית לה משוואה פשוטה - איזה משואה מהצורה $f(x, \dots, x_n) = 0$

ראשי f פתרון במקדמים שלמים. הניסוח הוא למציאת פתרונות בשלמים.

אנחנו רוצים לדעת אם יש פתרון או לא. ואם יש, אז כמה יש. אנחנו רוצים לדעת.

דוגמה: $x^2 + y^2 = z^2$ אנחנו רוצים שצדדים של משוואה יהיו אנטימים

אם המשוואה היא (x, y, z) השלמים המספרים שלמים שמקיימים את

הנכח הזה (קראו שלושה פיתגוראיים). למשל $(3, 4, 5)$, $(5, 12, 13)$

מה שצדדים של משוואה הוא שצדדים אנטימים. זהו הפתרון

האפשריים שלה. זאת משוואה הומוגנית. אם (x, y, z) שלושה פיתגוראיים

אז (mx, my, mz) שלושה פיתגוראיים לכל $m \in \mathbb{Z}$, לכן אנחנו רוצים

שלושה שאין להם חלק משותף

(המצומצמים)

לכן השלמים הפיתגוראיים הן מהצורה $(m^2 - n^2, 2mn, m^2 + n^2)$

עבור $m, n \in \mathbb{N}$ וראש $m \geq n$. $1 = (m, n)$ (כלומר הם זרים).

למשל $(3, 4, 5)$ מתקבלת - $n=1, m=2$.

הבעיה היא שלא כל המשוואות הן נחמדות ואפשר לתת פרימטיביות ולתת

של הפתרונות שלהן. דוגמה מפורסמת היא משוואה פרמה $x^n + y^n = z^n$.

המשפט האחרון של פרמה הוא שיש קיימים פתרונות שלמים לא טריוויאליים

למשוואה הזאת עבור $n \geq 3$. המשפט הזה הוכח על ידי ויליאם ויילס

הגדיר פלגון לקירובים דיאפנטים יהיה גשמה קצרה אחת. נשאל אם
 קיימת אחת שני חלקי הן לקבוע. גשמה נחשב פלגון δ .
 $x^p - y^q = 1$ עבור $p, q \geq 2$ ו- x, y שלמים. השערת קטלן היא
 שפלגון היחיד הוא $x=3, y=2$ אבל לא - כמו לא השערה. זה הוכח
 ו' איליאסקו.

שני המשפטים $x^n + y^n = z^n$ ו- $x^p - y^q = 1$ בן דמות. למעשה הן
 מהצורה $x^p + y^q = z^r$ - גשמה שנקראת גשמה פרמה-קטלן.
 הוכחה המעניין היא כאשר $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$ וזו עדין שאלה פתוחה.

כזה (חשבו לא על) $x^p - y^q = 1$ אז על $x^p - y^q = k$ עבור k קבוע
 גשמה המשווה אותה ל- x^p אקרה באינסוף רמה אך y^q
 החסמים הריציונליים צפופים בתוך החסמים הממשיים. אם $\varepsilon < \delta$ אז
 $x \in \mathbb{R}$ קיימים $p, q \in \mathbb{Z}$ כך ש- $|x - \frac{p}{q}| < \varepsilon$. למעשה, אם $x \in \mathbb{R}$
 אז $\frac{p}{q} \in \mathbb{Q}$ קיים $p \in \mathbb{Z}$ כך ש- $|x - \frac{p}{q}| \leq \frac{1}{2q}$. אינטואיטיבית,
 פשוט יש חלק, אך הישר חקטעים האורך $\frac{1}{q}$ ואז מציגים אותה x (וזה).
 פורמלית, נרשם $x = m + \alpha$ כאשר $m \in \mathbb{Z}$ ו- $0 < \alpha < 1$. ואז
 ניקח $P = \sum_{m=0}^m \alpha \leq \frac{1}{2}$ והם רמזים לקיים את הדיוט.
 אז נל- q קבוע הם ברור ה- p הגדלים הם ידוע ויחיד.
 שאלה יחיד מעניינת היא מה קורה ונשא מציגים את q .

משפט דיריכלט: אם $x \in \mathbb{R}$ אי-רציונלי קיימים אינסוף מספרים רציונליים
 $\frac{p}{q}$ כך ש- $|x - \frac{p}{q}| \leq \frac{1}{q^2}$.

המשפט הזה דיריכלט הוכיח בהנחה את עיקרון דיריכלט (או שובך הוזנים)
 שאומי שאלה מקסימים וזה כדורים δ -ח גאים אך יהיה תא שגבול
 ספחור 2 כדורים.

לדוגמה זאת, אם x רציונלי עם $\varepsilon < \delta$ קיים רק מספר סופי של רציונלים $\frac{p}{q}$
 כך ש- $|x - \frac{p}{q}| \leq \frac{1}{q^2}$.

זה נותן קריטריון לרציונליות של מספר.

②

הצגה: מספר $x \in \mathbb{R}$ נקרא איררציונלי מספר אם קיימים אינסוף מספרים רציונליים $\frac{p}{q}$ וקיים מספר קבוע $c > 0$ כן $\frac{c}{q^2} \leq |x - \frac{p}{q}|$.

לפי ההצגה זו משפט פיריארד אומר שכל מספר איררציונלי נקרא איררציונלי רציונליים מספר ≤ 2 . לעומת זאת אין מספר רציונלי שניתן לקרוא איררציונלי מספר $\leq 1 + \varepsilon$ עבור $0 < \varepsilon$.

נשים לב רק לרשומות $0 < \alpha \leq 1$ המעלה הכתובה היא המספר α עצמו.

הצגה: מספר x נקרא איררציונלי אם קיימים $a_1, \dots, a_n \in \mathbb{Q}$ כן $\frac{c}{q^2} \leq |x - \frac{p}{q}|$.
 $a_n = 0$, כלומר x היא שורש של פולינום מתוקן במקדמים רציונליים (או חתופין פולינום בשיעור המקדמים שלמים). מספר שאינו איררציונלי נקרא טרינסונדנטי. דוגמה מספר איררציונלי הם π והמספר e עבור $\frac{1}{q^2}$ פולינום $x^2 - 2$ הוא מספר רציונלי הוא איררציונלי $\sqrt{2}$ אינו רציונלי אבל לא איררציונלי.

נשים לב α רציונלי מהנקודה הזו קיימים מספרים איררציונליים לעומת טרינסונדנטיים.

משפט אינסקי: אם α הוא מספר איררציונלי אז $d > 1$ אז קיים c כן שיש רק מספר סופי של רציונליים $\frac{p}{q}$ כן $\frac{c}{q^d} \leq |x - \frac{p}{q}|$ (כלומר α לא נקרא איררציונלי מספר $\leq d$).

משפט רוג: מספר איררציונלי ≤ 2 , כלומר $0 < \varepsilon$ קיים רק מספר סופי של רציונליים $\frac{p}{q}$ כן $\frac{c}{q^2} \leq |x - \frac{p}{q}|$.

המספרים הם יחידים שניתן לקרוא איררציונלי הם המספרים מהצורה $\sqrt[n]{d}$.

פאלינגס הוויא משפט אינסקי: אם F פולינום הוויאני מצורה $x^2 + y^2 + z^2$ למשוואה $F(x, y, z) = 0$ תחת תנאים מסוימים קיים רק מספר סופי של פתרונות שלמים (כלומר $\frac{c}{q^2}$ הכפלה בסדר).

בפרט, עבור חקבונג למשוואה $x^2 + y^2 = z^2$ יש מספר סופי של פתרונות כאשר $z \geq n$ (זה דיון ארסטיא לא התנאים של המשפט).

הסדרה הקטנה:

Diophantine Analysis / Jörn Steuding

Invitation to Number Theory / S. Miller

השאלות הנשאלות:

- 1) משפטי הקירוב הקלאסיים - משפט דיריכלה, הורדז', קוונקר.
- 2) שברים משולבים
- 3) קירובים של מספרים ריבועיים
- 4) מספרים אלגבריים וטרנסצנדנטיים - משפט איזרוב, טרנסצנדנטיות
- 5) משפט דור (נושא מתקדם)

ד"ר חגית רמון

3d/10	ד"ר חגית רמון	משפטי קוונקר
6/11	ד"ר חגית רמון	קלאסיים
13/11	ד"ר חגית רמון	שברים משולבים
20/11	ד"ר חגית רמון	לוגיקה
27/11	ד"ר חגית רמון	מנהל

סני - ע'א 14-22 (אקדמי) בוליארי

uniform distribution or SC / NS

קא - ע'א 25-30 (Podé approximation)

1.12. For non-negative integers k , the **Fermat numbers** are defined by $F_k = 2^{2^k} + 1$.

Show that $\gcd(F_k, F_\ell) = 1$ for $k \neq \ell$. Deduce from this coprimality that there exist infinitely many prime numbers.

Fermat numbers are important with respect to the old question which regular n -gon can be constructed with ruler and compass (more details can be found in Section 9.6).

1.13.* From an algorithmic point of view it is sometimes an advantage to use a modified version of the Euclidean algorithm which works with the nearest integer.

Rewrite the Euclidean algorithm by replacing (1.11) by

$$r_{n-1} = q_{n+1}r_n + r_{n+1} \quad \text{with} \quad r_{n+1} \in \mathbb{Z}, \quad |r_{n+1}| \leq \frac{1}{2}|r_n|.$$

Show that this algorithm terminates, is at least as fast as the Euclidean algorithm, and also produces the greatest common divisor.

1.14. Prove that there are only finitely many best approximations $\frac{x}{y}$ to a given $\frac{a}{b} \in \mathbb{Q}$. Show that the best approximation with maximal y corresponds to the solution $x, y \in \mathbb{Z}$ of (1.12) with minimal $|y|$.

1.15. Using the Euclidean algorithm solve the linear diophantine equation

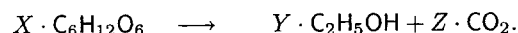
$$77\,708\,431X - 2\,640\,858Y = 1.$$

This provides a best approximation $\frac{p_1}{q_1}$ to $\frac{77\,708\,431}{2\,640\,858}$. Now continue these investigations for the linear equations $q_nX - p_nY = 1$ for $n = 1, 2, \dots$, where $\frac{p_n}{q_n}$ is the best approximation obtained by the preceding linear equation. Recover Huygens' approximation $\frac{206}{7}$ to $\frac{77\,708\,431}{2\,640\,858}$ from Section 1.8.

This provides an algorithm for finding the best approximations to a given rational number.

1.16. Write a computer program which computes the best approximations to a given real number below a given magnitude for the denominators. Use this to find the best approximations $\frac{p}{q}$ to π with $q < 10^7$.

1.17. From chemistry we know the fermentation reaction (important for producing alcohol) in the variables X, Y, Z :



Which quantities x, y, z for the ingredients can be chosen for this reaction?

1.18.* Find integral solutions x, y, z to the linear equation

$$17X - 11Y + 12Z = 1.$$

Classify all solutions! Show how to proceed with a linear diophantine equation in n variables.

Hint: Introducing a further variable W , investigate the system of linear equations $W = 17X - 11Y$ and $W + 12Z = 1$.

CHAPTER 2

Classical approximation theorems

So far we have proved only isolated results. Now it is time for theory! We start with the theory of diophantine approximations. In this chapter we shall prove classical theorems due to Dirichlet, Kronecker and Hurwitz and give some of their amazing applications (criteria for irrationality and uniform distribution). Further, with the pigeonhole principle and the Farey sequence we will learn two more simple but important tools in our diophantine toolbox.

2.1. Dirichlet's approximation theorem

It is much more interesting to approximate irrational numbers than rationals. As we have seen in Section 1.9, the set of best approximations to a given rational is finite. As we shall show now, the situation is rather different for irrational numbers.

In 1842, Dirichlet proved

Theorem 2.1. If α is irrational, then there exist infinitely many rational numbers $\frac{p}{q}$ such that

$$(2.1) \quad \left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2}.$$

This property characterizes irrational numbers; i.e., a rational α allows only finitely many approximations $\frac{p}{q}$ with (2.1).

The qualitative question whether a given real number α is irrational or not, depends on a quantitative property of α , namely, on the quality of rational approximations to α . Multiplying inequality (2.1) with q shows that, indeed, there are infinitely many best approximations to a given irrational α .

The following original proof of Dirichlet's approximation theorem relies on the so-called **pigeonhole principle** (or **box principle**) which states that if $n+1$ objects are distributed into n boxes, then at least one box contains at least two objects; this is easily seen by a contradiction argument or by induction.

Proof. We denote the **integral part** and the **fractional part** of a real number x by

$$[x] = \max\{z \in \mathbb{Z} : z \leq x\} \quad \text{and} \quad \{x\} = x - [x],$$

respectively; in some literature $[.]$ is also called **Gauss bracket**. Let Q be a positive integer. The numbers

$$0, \{\alpha\}, \{2\alpha\}, \dots, \{Q\alpha\}$$

define $Q + 1$ points distributed among the Q disjoint intervals

$$\left[\frac{j-1}{Q}, \frac{j}{Q} \right) \quad \text{for } j = 1, \dots, Q.$$

By the pigeonhole principle there has to be at least one interval which contains at least two numbers $\{k\alpha\} \geq \{\ell\alpha\}$, say, with $0 \leq k, \ell \leq Q$ and $k \neq \ell$. It follows that

$$\begin{aligned} \{k\alpha\} - \{\ell\alpha\} &= k\alpha - [k\alpha] - \ell\alpha + [\ell\alpha] \\ (2.2) \quad &= \{(k-\ell)\alpha\} + \underbrace{[(k-\ell)\alpha] + [\ell\alpha] - [k\alpha]}_{\in \mathbb{Z}}. \end{aligned}$$

Since $\{k\alpha\} - \{\ell\alpha\}$ lies in the interval $[0, \frac{1}{Q})$, the integral parts in (2.2) add up to zero. Setting $q = k - \ell$ we obtain

$$\{q\alpha\} = \{k\alpha\} - \{\ell\alpha\} < \frac{1}{Q}.$$

With $p := [q\alpha]$ it follows that

$$(2.3) \quad \left| \alpha - \frac{p}{q} \right| = \left| \frac{q\alpha - p}{q} \right| = \left| \frac{\{q\alpha\}}{q} \right| < \frac{1}{qQ},$$

which implies the estimate (2.1) (since $q < Q$).

Now suppose that α is irrational and that there exist only finitely many solutions $\frac{p_1}{q_1}, \dots, \frac{p_n}{q_n}$ to (2.1). Since $\alpha \notin \mathbb{Q}$, we can find a Q such that

$$\left| \alpha - \frac{p_j}{q_j} \right| > \frac{1}{Q} \quad \text{for } j = 1, \dots, n,$$

contradicting (2.3).

Finally, assume that α is rational, say $\alpha = \frac{a}{b}$ with $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. If $\alpha = \frac{a}{b} \neq \frac{p}{q}$, then

$$(2.4) \quad \left| \alpha - \frac{p}{q} \right| = \frac{|aq - bp|}{bq} \geq \frac{1}{bq},$$

and (2.1) involves $q < b$. This proves that there are only finitely many $\frac{p}{q}$ with (2.1). The theorem is proved. •

The proof is inefficient. Yet we cannot compute best approximations without big computational effort.

2.2. A first irrationality criterion

Dirichlet's approximation theorem leads to a first irrationality criterion.

Theorem 2.2. *If there are infinitely many coprime solutions p, q of*

$$(2.5) \quad \left| \alpha - \frac{p}{q} \right| < \frac{1}{q^{1+\delta}},$$

with a fixed $\delta > 0$, then α is irrational.

Proof. We assume that α is rational, say $\alpha = \frac{a}{b}$ with $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Then we shall show that both the set of p 's and the set of q 's satisfying (2.5) are finite. By contraposition, this gives the assertion of the theorem.

Combining (2.4) from the proof of Theorem 2.1 with (2.5) we get the inequality

$$\frac{1}{bq} < \frac{1}{q^{1+\delta}},$$

which implies that $q < b^{\frac{1}{\delta}}$. So there are only finitely many possible q 's. It remains to be shown that the same holds true for the p 's. For any given p, q with (2.5) we consider fractions of the form $\frac{p(t)}{q}$, where $p(t) = p + t$ with some integer variable t . If any of these fractions satisfies (2.5), it follows from the triangle inequality that

$$\frac{|t|}{q} = \left| \frac{t}{q} + \underbrace{\frac{p}{q} - \frac{a}{b}}_{=0} - \left(\frac{p}{q} - \frac{a}{b} \right) \right| \leq \left| \frac{p(t)}{q} - \frac{a}{b} \right| + \left| \frac{p}{q} - \frac{a}{b} \right| < \frac{2}{q^{1+\delta}}.$$

Thus, $|t| < 2q^{-\delta} \leq 2$ (since $q \geq 1$). Hence, for any one of the finitely many q 's there are at most three different values of t for which $p(t)$ can satisfy (2.5). So we are done. •

This simple criterion is surprisingly strong. For example,

$$(2.6) \quad \sum_{n=1}^{\infty} 10^{-n!} = 0.1100010000 \dots$$

is irrational. In order to prove this one only has to cut the series at one of the 1's which leads immediately to a candidate $\frac{p}{q}$ that satisfies (2.5) for some positive δ .

2.3. The order of approximation

We say that α is **approximable by rationals of order κ** if there exists a positive constant $c(\alpha)$, depending only on α , such that

$$\left| \alpha - \frac{p}{q} \right| < \frac{c(\alpha)}{q^{\kappa}}$$

has an infinity of rational solutions $\frac{p}{q}$. In a sense, κ indicates the speed of convergence of the "sequence" $\frac{p}{q}$ to α . Taking into account our previous observations we see that

- any rational α is approximable of order 1, and to no higher order (by Exercises 1.14 and Theorem 2.1);
- any irrational α is at least approximable of order 2 (by Theorem 2.1).

It is a natural question to ask for improvements of Dirichlet's theorem. Khintchine [90] proved in the 1930s a remarkable result which states that the set of numbers which allow a stronger approximation has **measure zero**; i.e., given any positive ε , the set can be covered by a countable number of intervals of total length less than ε .

Theorem 2.3. Suppose that ψ is a positive function such that

$$\sum_{q=1}^{\infty} \psi(q)$$

converges. Then for almost all α (i.e., the set of exceptional α has measure zero), there is only a finite number of solutions $p, q \in \mathbb{Z}$ to the inequality

$$(2.7) \quad |q\alpha - p| < \psi(q).$$

We are only interested in the fractional part of $q\alpha$, that is, the residue class of $q\alpha$ modulo $\mathbb{Z}$. For this purpose it is useful to represent numbers on a circle instead of on a straight line. In order to eliminate integral parts we may take the complex unit circle and represent a real number x by the point whose distance from 1 measured round the circumference in counter-clockwise direction is $2\pi x$. Then numbers which differ by an integer, as x and $\{x\}$, are represented by the same point of the circumference. This so-called **circular representation** automatically neglects the integer part $[x]$ of x . In other words, the mapping

$$x \mapsto \exp(2\pi ix)$$

is an isomorphism between the **circle group** $\mathbb{R}/\mathbb{Z}$ and the group of complex numbers of absolute value one.

Proof of Theorem 2.3. Given $\varepsilon > 0$, we can find an integer Q such that

$$\sum_{q \geq Q} \psi(q) < \frac{\varepsilon}{2}.$$

Without loss of generality we may restrict ourselves to numbers α lying in the interval $[0, 1)$. Consider those α for which the inequality (2.7) has infinitely many solutions. For each $q \geq Q$ consider the intervals of length $2\frac{\psi(q)}{q}$ centered around the rational numbers $\frac{0}{q}, \frac{1}{q}, \dots, \frac{q-1}{q}$ with respect to $\mathbb{R}/\mathbb{Z}$. Consequently, each α will lie in one of these intervals since

$$\left| \alpha - \frac{p}{q} \right| = \frac{|q\alpha - p|}{q} < \frac{\psi(q)}{q}.$$

The measure of these intervals is

$$\sum_{q \geq Q} q \cdot \frac{2\psi(q)}{q} < \varepsilon,$$

$$\{\alpha : \text{infinitely many solutions}\} \subseteq \bigcup_{q \geq Q} \left\{ \alpha : \left| \alpha - \frac{p}{q} \right| < \frac{\psi(q)}{q} \right\}$$

$$\sum_{q \geq Q} 2\psi(q) < \varepsilon$$

which proves the theorem. •

For example, we may take $\psi(q) = q^{-1}(\log q)^{-1-\varepsilon}$. Thus almost all numbers cannot be approximated by an order $2 + \varepsilon$. On the contrary, for a positive function ψ such that

$$\sum_{q=1}^{\infty} \psi(q)$$

diverges, Khintchine proved that for almost all α , there exist infinitely many solutions $p, q \in \mathbb{Z}$ to the inequality (2.7). A more subtle characterization of real numbers with respect to the order of approximation seems to be a rather difficult task.

2.4. Kronecker's approximation theorem

As we have seen above, for any given real α we can find integers q for which $q\alpha$ differs from an integer by as little as we please. Kronecker's celebrated approximation theorem from 1891 considers the inhomogeneous case.

Theorem 2.4. If α is irrational, $\eta \in \mathbb{R}$ is arbitrary; then for any $N \in \mathbb{N}$ there exist $Q \in \mathbb{N}$ with $Q > N$ and $P \in \mathbb{Z}$ such that

$$|Q\alpha - P - \eta| < \frac{3}{Q}.$$

$$\begin{aligned} N &= \frac{1}{10} \left[\frac{1}{\varepsilon} \right] \\ \eta &= \frac{3}{N} \end{aligned}$$

Proof. By Theorem 2.1 there are integers $q > 2N$ and p such that

$$|q\alpha - p| < \frac{1}{q}.$$

Suppose that m is the integer, or one of the two integers, for which

$$|q\eta - m| \leq \frac{1}{2}.$$

In view of Theorem 1.6 we can write $m = px - qy$, where x and y are integers and $|x| \leq \frac{1}{2}q$. Since

$$q(x\alpha - y - \eta) = x(q\alpha - p) - (q\eta - m),$$

we find

$$|q(x\alpha - y - \eta)| < \frac{1}{2}q \cdot \frac{1}{q} + \frac{1}{2} = 1.$$

Setting $Q = q + x$ and $P = p + y$ yields

$$N < \frac{1}{2}q \leq Q \leq \frac{3}{2}q,$$

and thus

$$|Q\alpha - P - \eta| \leq |x\alpha - y - \eta| + |q\alpha - p| < \frac{1}{q} + \frac{1}{q} = \frac{2}{q} \leq \frac{3}{Q}.$$

This is the inequality of the theorem. •

Kronecker's approximation theorem provides information on topological properties of sequences with respect to the circular representation. We start with dense sequences. A sequence of real numbers α_n is said to lie **dense** in an interval $[a, b]$ if for any open neighborhood U of any point of $[a, b]$,

there is an element $\alpha_n \in \mathcal{U}$. Recall that $\{\alpha_n\}$ denotes the fractional part of α_n , i.e., $\{\alpha_n\} = \alpha_n - [\alpha_n]$. By virtue of Kronecker's approximation theorem the sequence defined by $\alpha_n = \{n\alpha\}$ lies dense in $[0, 1)$ if and only if α is irrational. This gives another characterization of irrational numbers.

2.5. Billiard

Kronecker's approximation theorem has an interesting and entertaining consequence for billiard. This application is due to König & Szücs [93] and is known as the problem of the reflected light ray in plane geometry. The sides of a square are reflecting mirrors. A ray of light leaves a point inside the square and is reflected by the mirrors. What can be said about the path the ray of light will take?

Let γ be the angle between a side of the square and the initial direction. Without loss of generality we may assume that the square has edges of length 1, so we may think of the square as $[0, 1)^2 \subset \mathbb{R}^2$. The path of the ray of light is periodic if and only if the straight line is modulo $\mathbb{Z}^2$ the union of finitely many straight lines. On the contrary, the path is dense if the straight line lies dense in $(\mathbb{R}/\mathbb{Z})^2$. The straight line is given by

$$y = \alpha x + \beta,$$

where $\alpha = \tan \gamma$ and β is some real number.

First, assume that α is rational, say equal to $\frac{p}{q}$, where p and q are coprime integers. Consequently, this straight line is invariant under transformations

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x \\ y \end{pmatrix} + k \begin{pmatrix} q \\ p \end{pmatrix} \quad \text{for } k \in \mathbb{Z}.$$

Now assume that α is irrational. Given any point $(x_1, y_1) \in \mathbb{R}^2$ and any positive ε , Kronecker's approximation theorem, applied with $\eta = -y_1 + \beta + \alpha x_1$, yields integers P, Q such that

$$|y_1 + P - (\alpha(x_1 + Q) + \beta)| = |\underbrace{y_1 - \beta - \alpha x_1}_{=-\eta} + P - Q\alpha| < \varepsilon.$$

Hence, (x_1, y_1) and the point $(x_1, \alpha(x_1 + Q) + \beta)$ lie modulo $\mathbb{Z}^2$ as close as we please.



FIGURE 2.1. The way of reflected rays of light, one with an irrational tangent, the other one with a rational tangent.

Thus, the path of the ray of light is closed and periodic if and only if the angle between a side of the square and the initial direction of the ray has a rational tangent, that is, $\alpha = \tan \gamma \in \mathbb{Q}$; otherwise the ray of light passes arbitrarily near to every point of the square.

2.6. Uniform distribution

We say that a sequence $(\alpha_n)_n$ is **uniformly distributed modulo 1** if the proportion of the fractional parts $\{\alpha_n\}$ which lie in an arbitrary subinterval $[a, b)$ of $[0, 1)$ coincides with the length of $[a, b)$; more precisely, for any $0 \leq a < b < 1$,

$$\lim_{N \rightarrow \infty} \frac{1}{N} \#\{n \leq N : \{\alpha_n\} \in [a, b)\} = b - a.$$

The notion of uniform distribution has its origin in probability theory.

It is easy to see that a uniformly distributed sequence modulo 1 lies dense in $[0, 1)$ a fortiori. However, the converse implication does not hold: uniform distribution is a stronger concept than denseness. For instance, consider the sequence of the fractional parts of $\log n$, where here and in the sequel $\log n$ is the logarithm to base e . This sequence lies dense in $[0, 1)$ but it is easily seen that it is not uniformly distributed modulo 1. It is yet unproved whether the sequence of numbers $\exp(n)$ for $n \in \mathbb{N}$ is uniformly distributed modulo 1.

Theorem 2.5. *For irrational α , the sequence $(n\alpha)_n$ is uniformly distributed modulo 1.*

Proof. Let ε be a small positive quantity less than $\frac{1}{10}$. In view of Kronecker's theorem 2.4 there exists an integer m such that $0 < \{m\alpha\} =: \delta < \varepsilon$. Put $\Delta := [\frac{1}{\delta}]$ and, for $0 \leq d \leq \Delta$, define the intervals $\mathcal{I}_d$ by the inequalities

$$\{dm\alpha\} < x \leq \{(d+1)m\alpha\}.$$

The interval $\mathcal{I}_\Delta$ extends beyond the point 1, but we may use the circular representation. For $N \in \mathbb{N}$, denote by $\lambda_d(N)$ the number of $\{\alpha\}, \{2\alpha\}, \dots, \{N\alpha\}$, which lie in the interval $\mathcal{I}_d$. If $\{n\alpha\} \in \mathcal{I}_0$ for some positive integer n , then $\{(n+dm)\alpha\} \in \mathcal{I}_d$ and vice versa. Hence, for $N > dm$,

$$\lambda_d(N) - \lambda_d(dm) = \lambda_0(N - dm).$$

Obviously, $\lambda_d(dm) \leq dm$ and $\lambda_0(N - dm) \geq \lambda_0(N) - dm$. Therefore

$$\lambda_0(N) - dm \leq \lambda_d(N) \leq \lambda_0(N) + dm,$$

which implies

$$(2.8) \quad \lim_{N \rightarrow \infty} \frac{\lambda_d(N)}{\lambda_0(N)} = 1 \quad \text{for } 0 \leq d \leq \Delta.$$

Now

$$\sum_{d=0}^{\Delta-1} \lambda_d(N) \leq N \leq \sum_{d=0}^{\Delta} \lambda_d(N).$$

In view of (2.8) we get

$$(\Delta + o(1))\lambda_0(N) \leq N \leq (\Delta + 1 + o(1))\lambda_0(N), \quad \leftarrow$$

where as usual $f(x) = o(g(x))$ with a positive function $g(x)$ denotes that

$$\lim_{x \rightarrow \infty} \frac{|f(x)|}{g(x)} = 0.$$

It follows that

$$(2.9) \quad \frac{1}{\Delta + 1} \leq \liminf_{N \rightarrow \infty} \frac{\lambda_0(N)}{N} \leq \limsup_{N \rightarrow \infty} \frac{\lambda_0(N)}{N} \leq \frac{1}{\Delta}.$$

If $\mathcal{I} = [a, b)$ with $b - a \geq \varepsilon$, there exist positive integers u and v such that

$$0 \leq \{u\alpha\} \leq a \leq \{(u+1)\alpha\} \leq \{(u+v)\alpha\} \leq b < \{(u+v+1)\alpha\},$$

and

$$\sum_{d=u+1}^{u+v-1} \lambda_d(N) \leq N_{\mathcal{I}} \leq \sum_{d=u}^{u+v} \lambda_d(N),$$

where $N_{\mathcal{I}}$ is the number of $\{n\alpha\}$ with $n \leq N$ which fall into the interval $\mathcal{I}$, i.e.,

$$N_{\mathcal{I}} = \#\{n \leq N : \{n\alpha\} \in [a, b)\}.$$

By (2.8)

$$v - 1 \leq \liminf_{N \rightarrow \infty} \frac{N_{\mathcal{I}}}{\lambda_0(N)} \leq \limsup_{N \rightarrow \infty} \frac{N_{\mathcal{I}}}{\lambda_0(N)} \leq v + 1. \quad \downarrow$$

This gives in (2.9)

$$\frac{v-1}{\Delta+1} \leq \liminf_{N \rightarrow \infty} \frac{N_{\mathcal{I}}}{N} \leq \limsup_{N \rightarrow \infty} \frac{N_{\mathcal{I}}}{N} \leq \frac{v+1}{\Delta}.$$

Since

$$\delta\Delta \leq 1 \leq \delta(\Delta+1) \quad \text{and} \quad \delta(v-1) < b-a < \delta(v+1),$$

we deduce

$$\frac{b-a-2\delta}{1+\delta} \leq \liminf_{N \rightarrow \infty} \frac{N_{\mathcal{I}}}{N} \leq \limsup_{N \rightarrow \infty} \frac{N_{\mathcal{I}}}{N} \leq \frac{b-a+2\delta}{1-\delta}.$$

The quantities ε and δ can be chosen as small as we please; thus the theorem is proved. •

It is easy to see that $\sqrt{m}$ is rational if and only if m is a perfect square. Thus, Theorem 2.5 implies that the sequence $(n\sqrt{m})_n$ is uniformly distributed modulo 1 whenever m is not a perfect square.

Uniform distribution is an interesting subject with many important applications. For example, the Monte Carlo method for numerical integration relies on randomly chosen points in the range of integration in which the integrand in question is evaluated. If these points are uniformly distributed, the sum of these values is an approximate substitute for the integral. For this and more we refer the interested reader to Hlawka [83] or Kuipers & Niederreiter [96]. The city of Monte Carlo is famous for its elegant gambling casinos. The name Monte Carlo method is a tribute to the celebration of the *laws of chance* played there.

2.7. The Farey sequence

The Farey sequence was introduced by Haros in 1802 and (independently) by Farey in 1816. However, Cauchy was the first who studied it systematically.

For any positive integer n the **Farey sequence $\mathcal{F}_n$ of order n** is the ordered list of all reduced fractions in the unit interval having denominators $\leq n$:

$$\mathcal{F}_n = \left\{ \frac{a}{b} \in \mathbb{Q} : 0 \leq a \leq b \leq n \text{ with } (a, b) = 1 \right\}.$$

For example,

$$(2.10) \quad \mathcal{F}_1 = \left\{ \frac{0}{1}, \frac{1}{1} \right\} \subset \mathcal{F}_2 = \left\{ \frac{0}{1}, \frac{1}{2}, \frac{1}{1} \right\} \subset \mathcal{F}_3 = \left\{ \frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1} \right\} \subset \dots$$

Clearly, $\mathcal{F}_n \subset \mathcal{F}_{n+1}$ (here we wrote the new members in bold face). Each rational in the unit interval will eventually occur in the Farey sequence, and hence the Farey sequence is building $\mathbb{Q}$ modulo $\mathbb{Z}$. In particular, this construction proves once more that $\mathbb{Q}$ is countable.

How large is $\mathcal{F}_n$? The number of Farey fractions in $\mathcal{F}_n$ is related to **Euler's totient** $\varphi(b)$ which counts the number of positive coprime integers $a \leq b$, i.e.,

$$\varphi(b) = \#\{1 \leq a \leq b : \gcd(a, b) = 1\}.$$

Before we answer the question on the size of $\mathcal{F}_n$ we introduce the useful **Landau-Vinogradov symbols**. We write

$$f(x) = O(g(x)) \quad \text{and} \quad f(x) \ll g(x),$$

respectively, where $g(x)$ is a positive function, if

$$\limsup_{x \rightarrow \infty} \frac{|f(x)|}{g(x)} \text{ is bounded,}$$

or equivalently, if there exists a positive constant C such that $|f(x)| \leq Cg(x)$ for all sufficiently large x . Using this notation and with some knowledge on arithmetic functions one can prove the asymptotic formula

$$(2.11) \quad \#\mathcal{F}_n = 1 + \sum_{b \leq n} \varphi(b) = \frac{3}{\pi^2} n^2 + O(n \log n).$$

Thus, $\mathcal{F}_n$ is growing quadratically in n .

Two consecutive elements in $\mathcal{F}_n$ are called **neighbors**. Of course, this relationship breaks down as $n \rightarrow \infty$. Nevertheless, neighborhood is a fundamental concept in the theory of Farey fractions.

Theorem 2.6. For any neighbors $\frac{a}{b} < \frac{c}{d}$ in $\mathcal{F}_n$,

$$bc - ad = 1.$$

In particular, under the assumptions of the theorem

$$\frac{c}{d} - \frac{a}{b} = \frac{bc - ad}{bd} = \frac{1}{bd}.$$

הגדרה: $n \in \mathbb{N}$ נקרא f_n פונקציה n -מרחבית אם $f_n: \mathbb{R}^n \rightarrow \mathbb{R}$ היא פונקציה רציפה, $f_n(0) = 1$ ויש לה נקודת מינימום $f_n(a) = 0$ עבור $a \in \mathbb{R}^n$.

$$f_1 = \left\{ \frac{0}{1}, \frac{1}{1} \right\}, \quad f_2 = \left\{ \frac{0}{1}, \frac{1}{2}, \frac{1}{1} \right\}$$

$$f_3 = \left\{ \frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1} \right\}$$

① סדרנו של $n \in \mathbb{N}$ $f_n \subseteq f_{n+1}$ (האיברים הנוספים הם אלה שאינם החדים) $(n+1)$

$$f_n \text{ פונקציה } (n \in \mathbb{N}) \text{ מ } \mathbb{R} \text{ ל } \mathbb{R} \text{ (היא) } (2)$$

$n > N$ bđ $x \in I_n$ v $n \in \mathbb{N}$ sđ $x \in \mathbb{Q} \cap [0, 1]$ bđ ③

וזה מקום אחרון אלהים נוסף להצטרף הם קבוצה
בת אחת (איש לקבוצה הסדרה Farey בת אחת)

1. $f(x) = O(g(x))$ כחמה גדולה
 2. $f(x) \ll g(x)$ חסומה
 3. $\limsup_{x \rightarrow \infty} \frac{|f(x)|}{g(x)}$

זרז מוסר $\mathcal{E}$ (שמשלבו בו היא פונקציה φ לא אוויר :
 $\varphi(b) = |\{1 \leq a \leq b : (a,b) = 1\}|$

(ג) הִיא מספר החסמים שלמים b (קטנים ממני).
כן, למשל $\varphi(p) = p - 1$

$\varphi(ab) = \varphi(a)\varphi(b)$ וכן $(a,b) = 1$ מכלל תכונה של φ

$$\text{gic} \quad h = p_1^{k_1} \dots p_r^{k_r} \quad \text{r/c} \quad \text{gic}$$

$$\varphi(n) = \varphi(p_1^{k_1}) \cdots \varphi(p_r^{k_r})$$

$$K = \{ p \in P \mid \varphi(p^k) \text{ is a prime} \}$$

דמיון, עבור p^2 המספרים היוצאים שלהם מתחלקים
 בהם זהו הכפול של p . $\Leftrightarrow \psi(p^2) = p^2 - p$
 באופן כללי עבור p^k $\psi(p^k) = p^k - p^{k-1}$ משום
 של p^k יש $\frac{p^k}{p}$ מספרים שלהם מתחלק ב p .

$$\Rightarrow \psi(n) = \prod_{i=1}^r (p_i^{k_i} - p_i^{k_i-1}) = \prod_{i=1}^r (1 - \frac{1}{p_i}) \cdot n$$

זה נחזור ל- f_n . אם יש לנו את f_n רציף ארבעה אר
 ו f_{n+1} אנתנו אחרים אלוסוף את השלבים המצומצמים עם
 מכנה וחד. $\Leftrightarrow$ אנתנו אוספים $\psi(n+1)$ שלבים.
 באופן כללי:

$$|f_n| = 1 + \sum_{b \leq n} \psi(b) = \frac{3}{\pi^2} n^2 + O(n \log n)$$

כלומר f_n גדלה בקצב ריבועי.

אפשר לחשוב על זה קצת אחרת - אם היינו לוקחים את
 ב הזוגות (a, b) עבור $a \leq a \leq b \leq n$ היינו מקבלים
 $\frac{n(n-1)}{2} = \binom{n}{2}$, שזה משהו ריבועי. אבל אנתנו צריכים לא
 את ב הזוגות אלא רק את הלחים, אז הקבוצה קטן...

הצדקה: שני שלבים $\frac{a}{b} < \frac{c}{d}$ יוקראו שלבים אם הם אינם
 עוקבים ב- f_n עבור n מספיק גדול.

נשים לב שתכונה זו לא נשמרת כאשר $n \rightarrow \infty$, לכן אם
 n גדול אז אנתנו מכניסים כצירוף בין $\frac{a}{b}$ ל- $\frac{c}{d}$ כלומר
 אין כצירוף שיש להם שלבים ענדה.

משפט: אם $\frac{a}{b}, \frac{c}{d}$ שלבים מתקיים $bc - ad = 1$ אז
 $\frac{c}{d} - \frac{a}{b} = \frac{bc - ad}{bd} = \frac{1}{bd}$

תכונה של סדרה Farey לאנכות: הסדרה f_n מתפזרת
 באופן אחיד אופטו 1.

9

משפט התפוצה הראשון:

יהי $\pi(x)$ מספר המספרים הראשוניים $\leq x$.

$$\pi(x) = \int_2^x \frac{du}{\log u} + O\left(x \exp\left(-\frac{\log^{3/5} x}{\log \log \frac{1}{5}}\right)\right)$$

זאת נקראת תוצאה חזקה.

השערה רימן - ל- $x^{\frac{1}{2}+\epsilon}$ $\pi(x) - \int_2^x \frac{du}{\log u} \ll$ עבור $0 < \epsilon$.

וכך שקלף לריק - ל- $n^{\frac{1}{2}+\epsilon}$ $\sum_{j=1}^{|\mathcal{P}_n|-1} \left| \frac{1}{p_j} - \frac{1}{|\mathcal{P}_n|-1} \right| \ll$

(יחס שבתוספת הכי אופטימלי (כא $x^{\frac{1}{2}}$ אבל לא הוכח
שהוא הטוב ביותר...)

הוכחת המשפט מהצמוד הקודם:

למה: המשוואה $bx - ay = c$ בתורה אנטי (a,b) מחלק
א-כ ו- $n-b < y \leq n$ (*)

יתר, (תן ל- $(a,b)=1$ רק משוואה $bx - ay = 1$
יש פתרונות $x, y \in \mathbb{N}$ $\iff (x,y)=1 \iff (a,b)=1$ $\iff \frac{x}{y} \in \mathcal{F}_n$

$$\Rightarrow \frac{x}{y} - \frac{a}{b} = \frac{bx - ay}{by} = \frac{1}{by}$$

נניח ל- $\frac{x}{y} - \frac{c}{d} = \frac{dx - cy}{dy} \geq \frac{1}{dy}$ וכן $\frac{a}{b} < \frac{c}{d} < \frac{x}{y}$

כמו כן, $\frac{c}{d} - \frac{a}{b} = \frac{cb - ad}{db} \geq \frac{1}{db}$

$$\Rightarrow \frac{x}{y} - \frac{a}{b} = \frac{x}{y} - \frac{c}{d} + \frac{c}{d} - \frac{a}{b} \geq \frac{1}{dy} + \frac{1}{db} = \frac{d+b}{dby} \stackrel{(*)}{\geq} \frac{n}{dby}$$

$d > n \iff \frac{x}{y} - \frac{a}{b} > \frac{n}{dby} \iff \frac{x}{y} - \frac{a}{b} = \frac{1}{by}$ for

$\frac{c}{d} \notin \mathcal{F}_n \iff$ קיבלנו סתירה! $\frac{a}{b}, \frac{c}{d}$ הם שברים.

⊙

$\frac{c}{d} = \frac{x}{y} \iff$ ומקיים הפתור.

חזשן אנחנו יורלם אלהיז מתי לטמי $\frac{a}{b} < \frac{c}{d}$ מאמרים
אל תכונת הולתם לטמי.

משפט: שני לטמי $\frac{a}{b}, \frac{c}{d}$ חוקים ב-אז מאמרים את תכונת
הלכנות לראשונה ב- n ואלר $n = b+d$.

הולתה: (סתב φ) המשפר $\frac{a+c}{b+d}$ קל לוראל ל-
 $\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}$ (נשים אל ל"ממוצ" הזה הוא ל-
מנוטוני. למד $\frac{1}{3} > \frac{1}{6}$; $\frac{2}{3} > \frac{23}{36}$ אמד

$$\left(\frac{1+23}{6+36} = \frac{4}{7} > \frac{1}{2} = \frac{1+2}{3+3} \right)$$

אנחנו רוצים להוראל ללא נקס איבר באמצע לפני $n = b+d$.

ע"ם המשפט הקודם אל יש לטמי $\frac{a}{b} < \frac{x}{y} < \frac{c}{d}$ אז

$$\begin{aligned} dbx - day = d &\Leftrightarrow bx - ay = 1 &\Rightarrow bcx - acy = c \\ bcy - bxd = b &\Leftrightarrow cy - xd = 1 &\Rightarrow \underline{acy - axd = a} \end{aligned}$$

$$y(bc - ad) = b + d$$

$$x(bc - ad) = a + c$$



$$\frac{x}{y} = \frac{x(bc - ad)}{y(bc - ad)} = \frac{a + c}{b + d}$$

האנו שאל הכנסנו רק אבר אחד בין $\frac{a}{b}$ ל- $\frac{c}{d}$ אז האובר

הזה היא $\frac{a+b}{c+d}$. למה לא יורל להיות לפני $n = c+d$

הכנסנו שני אברים חדשים בין $\frac{a}{b}$ ל- $\frac{c}{d}$?

הסיבה היא לביטאונתנו זוכרים ל- n ו- n ל- n מוספים רק

איברים ע"ם מכנה n . אז נניח שיש שטמים:

$$\frac{a}{b} < \frac{x}{n} < \frac{x+y}{n} < \frac{c}{d}$$

אם אז $ny = n(x+y) - nx = 1$ וזה לא יורל להיות!

כמו כן, יש זלום ל המשפר $\frac{a+c}{b+d}$ הוא מצומצם.



החסידים מבינים היקףם וזאת שגורם להם

ה. בציורה אינפיקטיוס "ח $f_1 = \left\{ \frac{0}{1}, \frac{1}{1} \right\}$

אם יש גר f_{n-1} עובדים ב סוג שונים. אם סכום
המקרים שלהם יהיו n אז צריך להוסיף את הממוצע שלהם
 $f_n - f$.

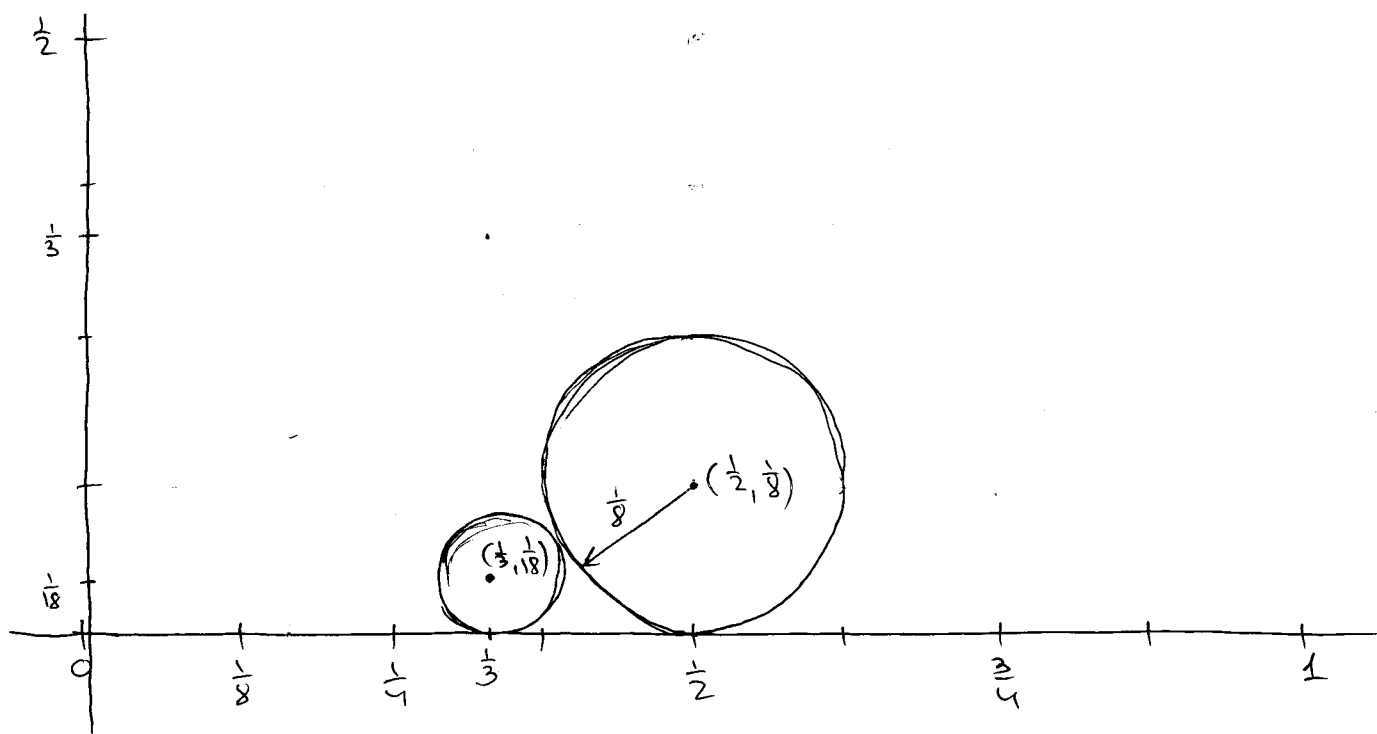
ford, from

נחתם את קצת היותה פאישור, ומכאן C ונצור

$$\therefore \frac{a}{b} \in \mathbb{F}_n \quad \text{Bf}$$

$$C\left(\frac{a}{b}\right) = \left\{ z \in \mathbb{C} : \left| z - \left(\frac{a}{b} + \frac{i}{2b^2} \right) \right| = \frac{1}{2b^2} \right\}$$

זה משהו בן 1700 סמים הנקראים $(\frac{a}{b}, \frac{1}{2b^2})$



unik pnnj $C(\frac{a}{b})$, $C(\frac{c}{d})$ for all a, b, c, d in $\mathbb{N}$

הם משקלים $\frac{a}{b}, \frac{c}{d}$ ביניים.

האומה: נמצא את נמחק בין שני אנשי המעשים

$$d^2 = \left(\frac{a}{b} - \frac{c}{d} \right)^2 + \left(\frac{1}{2b^2} - \frac{1}{2d^2} \right)^2$$

$S = \frac{1}{2b^2} + \frac{1}{2d^2}$ = הרקדיוסים $S = r_1 + r_2$ (10)

$$d^2 - s^2 = \left(\frac{a}{b} - \frac{c}{d}\right)^2 - \frac{1}{b^2 d^2} =$$

$$= \frac{(ad-bc)^2 - 1}{b^2 d^2} = 0$$

לפי $\frac{a}{b} < \frac{c}{d}$ נניח $ad-bc=1$ נניח $\frac{a}{b} < \frac{c}{d}$ נניח

האחרת של שניהם של השברים אפשר לראות שזה

$$bc - ad = 1 \quad \frac{a}{b}, \frac{c}{d} \text{ שונים}$$

אם נהיה להם רצון הוא אמנם.

⊙

נחזור לקירובים של מספרים רציונליים.

אם α איננו רציונלי לפי משפט פירייה קיימים אינסופים רציונליים $\frac{p}{q}$ כך ש- $|\alpha - \frac{p}{q}| \leq \frac{1}{q^2}$, באופן $|\alpha - \frac{p}{q}| \leq 1$ בקלות קטן יותר.

נסתב על יחס הזה $G = \frac{1}{2}(\sqrt{5}+1)$. דרך אחרת לקבוע אותו היא ד"ר מנהל של אינפניטסזים של סדרת פיבונאצ'.

$$\frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8} \longrightarrow G$$

במקרה זה $0.447 \dots \rightarrow |\alpha - \frac{p}{q}| < \frac{1}{q^2}$ אז אפשר לומר קרוב.

משפט Hurwitz: אם α איננו רציונלי אזי קיימים אינסוף

רציונליים $\frac{p}{q} \in \mathbb{Q}$ כך ש- $|\alpha - \frac{p}{q}| < \frac{1}{\sqrt{5}q^2}$ וכן, $\sqrt{5}$ הקבוע הטוב ביותר. באופן, אם $\sqrt{5}$ יוחזר בקלות גדול

ממנו אז יש מספר סופי של פתרונות רציונליים עבור $\alpha = G$.

הנחה: נניח ש- $\frac{a}{b} < \frac{c}{d}$ שניהם - $\frac{a}{b}$ ו- $\frac{c}{d}$ (אחרת ניקח $1-\alpha$)
 $\frac{a}{b} < \alpha < \frac{c}{d}$. נניח בהתאמה $\alpha > \frac{a+c}{b+d}$ (אחרת ניקח $1-\alpha$)
 נניח בשלילה -

$$\alpha - \frac{a}{b} \geq \frac{1}{\sqrt{5}b^2}$$

$$\alpha - \frac{a+c}{b+d} \geq \frac{1}{\sqrt{5}(b+d)^2}$$

$$\frac{c}{d} - \alpha \geq \frac{1}{\sqrt{5}d^2}$$

11) אם נניח שמתקיים אי-שוויון אחד מהאי-שוויונים האלה אז
 מקיים נוסף מכנינו האי-שוויון $\frac{a}{b} \geq \frac{1}{\sqrt{5}}$ למתקנת $a-b$.
 (וגם שיש סתירה)

$$\frac{c}{d} - \frac{a}{b} \geq \frac{1}{\sqrt{5}} \left(\frac{1}{b^2} + \frac{1}{d^2} \right)$$

$$\frac{c}{d} - \frac{a+c}{b+d} \geq \frac{1}{\sqrt{5}} \left(\frac{1}{d^2} + \frac{1}{(b+d)^2} \right)$$

דפי משפט ק'3

$$\frac{c}{d} - \frac{a}{b} = \frac{1}{bd}, \quad \frac{c}{d} - \frac{a+c}{b+d} = \frac{1}{d(b+d)}$$

$$\Rightarrow \sqrt{5} bd \geq b^2 + d^2$$

$$\sqrt{5} (d^2 + abd) \geq 3d^2 + 2bd + ab^2$$

$$\Rightarrow 0 \geq 4b^2 - 4(\sqrt{5}-1)bd + (5-2\sqrt{5}+1)d^2$$

$$\Rightarrow 0 \geq (2b - (\sqrt{5}-1)d)^2$$

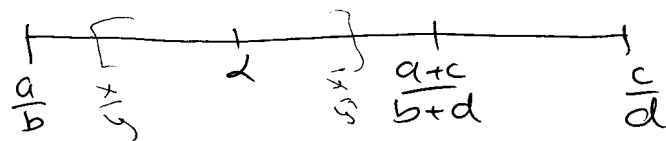
$$\Rightarrow 2b - (\sqrt{5}-1)d = 0$$

ולכן סתירה כי $\sqrt{5}$ אי-רציונלי ואילו $bd \in \mathbb{Z}$

← חתכו
 והסתבר
 אי-אפשר

$$\frac{c}{d} - a < \frac{1}{\sqrt{5}d^2} \quad \text{או} \quad a - \frac{a}{b} < \frac{1}{\sqrt{5}b^2} \quad \text{או} \quad a - \frac{a+c}{b+d} < \frac{1}{\sqrt{5}(b+d)^2} \quad \Leftarrow$$

עדיין יש לנו את המצב הנ"ל:



אחד מהקטעים האלה מקיים את האי-שוויון. אם נוסף לקחת
 סביב a קטע קטן $\frac{1}{\sqrt{5}(b+d)^2}$ ונתייחס אליו כרציונליים
 $\frac{x}{y}, \frac{x'}{y'}$ שהם מסביב a והם שברים האי-שליו $\frac{1}{2}$.
 זה שם יוצר לנו את הממוצע $\frac{x+x'}{y+y'}$ וזהו אי-התאמה.
 הנה אפשר להראות אינסוף פעמים.

נותר להוכיח ש- $\sqrt{5}$ (יש הקטנות) והכי טוב לבדוק $\dots$

12) 13.11.04

תורת
המספרים

שיעור 48 חז"י

לברית משולבים Continued Fractions

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots \frac{1}{a_n}}}$$

לבר משולב סופי היא מבצרה
ב ה- a_i חסמים פרט אולי
ס- a_0 .

אם ב ה- a_i שלמים קראים לבר לבר משולב פשוט.

משפט 1 ב $\frac{p}{q}$ רציונלי נותן להצגה רבר משולב פשוט.
הוכחה: (תוך 48 שארית)

$$0 < r_1 < q \quad p = a_0 q + r_1$$

$$0 < r_2 < r_1 \quad q = a_1 r_1 + r_2$$

$$\vdots$$

$$r_{n-1} = a_n r_n$$

התהליך הזה חייב להיגמר כי הסדרה $r_1, r_2, \dots$ יורדת
אין מהמשוואה האחרונה לקבלים את ההצגה הנמוק שלה?

$$p = a_0 q + r_1 \Rightarrow \frac{p}{q} = a_0 + \frac{r_1}{q}$$

$$q = a_1 r_1 + r_2 \Rightarrow \frac{q}{r_1} = a_1 + \frac{r_2}{r_1}$$

$$\vdots$$

$$r_{n-1} = a_n r_n \Rightarrow \frac{r_{n-1}}{r_n} = a_n$$

אזכורו (וב) אלה את ה- הוכחה:

$$\frac{p}{q} = a_0 + \frac{r_1}{q} = a_0 + \frac{1}{a_1 + \frac{r_2}{r_1}} =$$

$$= a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{r_3}{r_2}}} = \dots = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots \frac{1}{a_{n-1} + \frac{1}{a_n}}}}$$



זהו לא נעים לכתוב את השבר כמו שהוא אלא נכתוב

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots a_{n-1} + \frac{1}{a_n}}}} = [a_0; a_1, a_2, \dots, a_n]$$

ההצגה היא לא יחידה! (שם זה של מתקנים)

$$a_{n-1} + \frac{1}{a_n} = a_{n-1} + \frac{1}{a_{n-1} + \frac{1}{1}}$$

$$[a_0; a_1, a_2, \dots, a_n] = [a_0; a_1, \dots, a_{n-1}, a_{n-1} + \frac{1}{a_n}, 1]$$

אז אפשר לראות שיש הבדל בין ההצגה והיחידה!

דוגמה: (חשב את $365 + \frac{419}{1730}$ שזה מספר הימים בשנה)

$$1730 = 4 \cdot 419 + 54$$

$$419 = 7 \cdot 54 + 41$$

$$54 = 1 \cdot 41 + 13$$

$$41 = 3 \cdot 13 + 2$$

$$13 = 6 \cdot 2 + 1$$

$$2 = 2 \cdot 1$$

$$\Rightarrow 365 + \frac{1}{4 + \frac{1}{7 + \frac{1}{1 + \frac{1}{3 + \frac{1}{6 + \frac{1}{2}}}}}} =$$

$$= [365; 4, 7, 1, 3, 6, 2]$$

נשים לב שאת חותכים את השבר והמשק איפשרו באמצע

אם מקבלים קירוב של המספר המקורי. קירוב שלקראת אנה חלקי...
אם אנחנו $365 + \frac{1}{4}$ זה קירוב של מספר הימים בשנה. ואכן
פזם בארבע שנים יש לנו שנה מעוברת (בדיוק...)

$$[a_0; a_1, \dots, a_{n-1}, a_n] = [a_0; a_1, \dots, a_{n-1} + \frac{1}{a_n}]$$

אם צע' מן רכר לא נהנה שבר משק פשוט, אבל זה בס' לא שכן.

$$C_n = [a_0; a_1, \dots, a_n]$$

הצגה: האנה החלקי ה- n עבור $n \leq m$ הם

$$p_{-1} = 1$$

$$p_0 = a_0$$

$$p_n = a_n p_{n-1} + p_{n-2}$$

$$q_{-1} = 0$$

$$q_0 = 1$$

$$q_n = a_n q_{n-1} + q_{n-2}$$

לדיוק זה שני סדרות:

עבור $0 \leq n \leq m$

13

$$C_n = \frac{p_n}{q_n} \quad \text{משפט}$$

הוכחה: באינדוקציה על n .

$$\frac{p_0}{q_0} = \frac{a_0}{1} = a_0 \quad ! \quad C_0 = [a_0] = a_0$$

עבור $n=0$ מתקיים

נניח שהמשפט נכון עבור n :

$$C_n = [a_0; a_1, \dots, a_n] = \frac{p_n}{q_n} = \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}}$$

וכך נלכת - $n+1$:

$$\begin{aligned} C_{n+1} &= [a_0; a_1, \dots, a_n, a_{n+1}] = [a_0; a_1, \dots, a_n + \frac{1}{a_{n+1}}] = \\ &\stackrel{**}{=} \frac{(a_n + \frac{1}{a_{n+1}}) p_{n-1} + p_{n-2}}{(a_n + \frac{1}{a_{n+1}}) q_{n-1} + q_{n-2}} = \frac{(a_{n+1} a_n + 1) p_{n-1} + a_{n+1} p_{n-2}}{(a_{n+1} a_n + 1) q_{n-1} + a_{n+1} q_{n-2}} = \\ &= \frac{a_{n+1} (a_n p_{n-1} + p_{n-2}) + p_{n-1}}{a_{n+1} (a_n q_{n-1} + q_{n-2}) + q_{n-1}} = \frac{a_{n+1} p_n + p_{n-1}}{a_{n+1} q_n + q_{n-1}} = \frac{p_{n+1}}{q_{n+1}} \end{aligned}$$

😊

שאלה אחת: (ראה טבלה) השתמשו בהוכחה כדי להוכיח $p_{n-1} q_n - p_n q_{n-1} = (-1)^n$.

$$\begin{aligned} p_1 &= a_0 a_1 + 1 \\ q_1 &= a_1 \end{aligned} \Rightarrow \frac{p_1}{q_1} = a_0 + \frac{1}{a_1} = [C_1]$$

העניין הוא להי נוסחאות באינדוקציה משתמשות בשני שלבים
אחרים. $\Leftarrow$ חייבים לבדוק שני חסוים אינדוקציה ואנחנו פשוט לבחנו
עצמנו את זה! אז ערשנו עשינו והם מסודר...

$$\text{משפט: } p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1} \quad \text{בזמן } \frac{p_{n+1}}{q_{n+1}}, \frac{p_n}{q_n} \text{ שבתים (עוקבים באינדוקציה). (Farey)}$$

הוכחה: באינדוקציה על n :

$$a_0 \cdot 0 - 1 \cdot 1 = (-1)^{-1} \quad \text{עבור } n=0 \text{ מתקיים}$$

$$(a_0 a_1 + 1) \cdot 1 - a_1 a_0 = 1 = (-1)^0 \quad \text{עבור } n=1 \text{ מתקיים}$$

נניח שהמשפט נכון עבור n ונלכת - $n+1$:

$$\begin{aligned} p_{n+1} q_n - q_{n+1} p_n &= (a_{n+1} p_n + p_{n-1}) q_n - (a_{n+1} q_n + q_{n-1}) p_n = \\ &= p_{n-1} q_n - q_{n-1} p_n = -(p_n q_{n-1} - p_{n-1} q_n) = -(-1)^{n-1} = (-1)^n \end{aligned}$$

😊

נשים לרוב שגם המשפטים זהו לא השתמשו בהם ל- α_i שלמים
 ואם הם נכונים גם הם לא שלמים.

אם, אם הם לא שלמים אז ה- p_i ו- q_i שלמים
 ואם אחד של $(-1)^{n-1} = p_n q_{n-1} - q_n p_{n-1}$ נובע ל- p_n ו- q_n זרים, סומך
 $(p_n, q_n) = 1$ אם $\frac{p_n}{q_n}$ שבר מצומצם.
 חלף משה, נשים לב גם ל- p_n ו- q_n סדרות עולה, זמנא, הן עולה
 לפחות כמו סדרת פיבונצ'.

משפט שני: חזרת הקדמה:
 $p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1}$

$$\frac{r_{n-1}}{r_n} = q_n + \left(\frac{r_n}{r_{n+1}}\right)^{-1}$$

$$\begin{array}{lll} p_{-1} = 1 & p_0 = a_0 & p_n = a_n p_{n-1} + p_{n-2} \\ q_{-1} = 0 & q_0 = 1 & q_n = a_n q_{n-1} + q_{n-2} \end{array}$$

$$C_n = \frac{p_n}{q_n}$$

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_n q_{n-1}}$$

משפט:

- (א) המונה והמכנה של אפיקס בלוי הן סדרה עולה ממל
- (ב) המונה והמכנה של אפיקס איזוי הן סדרה יורדת ממל
- (ג) אם מנה חלקי-המכנה של אפיקס בלוי קטנה אם מנה חלקי-המכנה של אפיקס איזוי.

הוכחה:
 $C_{n+2} - C_n = (C_{n+2} - C_{n+1}) + (C_{n+1} - C_n) =$

$$= \frac{(-1)^{n+1}}{q_{n+2} q_{n+1}} + \frac{(-1)^n}{q_{n+1} q_n} = \frac{q_n (-1)^{n+1} + q_{n+2} (-1)^n}{q_n q_{n+1} q_{n+2}} =$$

$$= \frac{(-1)^n (q_{n+2} - q_n)}{q_n q_{n+1} q_{n+2}} = \frac{(-1)^n a_{n+2} q_{n+1}}{q_n q_{n+1} q_{n+2}} = \frac{(-1)^n a_{n+2}}{q_n q_{n+2}}$$

המנה $\frac{a_{n+2}}{q_n q_{n+2}}$ היא תמיד חיובית אם a_{n+2} חיובית (אם $(-1)^n$).

אם $C_n < C_{n+2}$ ואם $C_n > C_{n+2}$ אז C_n איזוי אם $C_n > C_{n+2}$.

נותר להוכיח את (ג). מתקיים
 $C_{n+1} - C_n = \frac{(-1)^n}{q_{2n+1} q_{2n}} = \frac{1}{q_{2n+1} q_{2n}}$

(ד) $C_{ab} < C_{ab+2a} < C_{2a+2b+1} < C_{2a+1}$
 (האיזויים יוצאים)



(עבור שלבים משולבים אינסופיים)

הצדקה: בהינתן סדרה אינסופית $(a_n)_{n=0}^{\infty}$ של שלמים שליליים או לא-שליליים a_0 חזריים (יציור שלם המשלב האינסופי):

$$[a_0; a_1, a_2, \dots, a_n, \dots] = \lim_{n \rightarrow \infty} [a_0; a_1, a_2, \dots, a_n]$$

משפט: בהנחות הנ"ל α הסדרה היחידה קיים והוא מספר אי-רציונלי.

הוכחה: ראוי ש- C_n סדרה מונוטונית עולה וחסומה מעלית ע"י C_1

ולכן היא מתכנסת. אם C_{n+1} סדרה מונוטונית יורדת וחסומה מעלית

ע"י C_0 ולכן מתכנסת. נסמן $\alpha = \lim C_n$ ו- $\alpha' = \lim C_{n+1}$.

מה שאנחנו רוצים להוכיח הוא למעלה ש- $\alpha = \alpha'$.

ברור ש- $\alpha \leq \alpha'$. מצד שני, $\alpha' - \alpha < C_{n+1} - C_n = \frac{1}{q_{2n+1}q_{2n}} \rightarrow 0$

$\Leftrightarrow \alpha = \alpha'$ (הצדקה קיים ונסמנו ב- α).

(נראה כי זה ש- α אי-רציונלי).

$$(*) \quad \left| \alpha - \frac{p_k}{q_k} \right| = \left| \alpha - C_k \right| < |C_{k+1} - C_k| = \frac{1}{q_{k+1}q_k} < \frac{1}{q_k^2}$$

היחלף ש- $\dots < C_5 < C_3 < C_1$ ו- $C_0 < C_2 < C_4 < \dots$

נחס שבה- C_k שונים, סומרי סה- $\frac{p_k}{q_k}$ שונים. $\Leftrightarrow$ קיבלנו ש- $(*)$

יש מספר אינסופי של פתרונות $\Leftrightarrow$ לפי משפט דיריכלה α הוא אי-רציונלי.

(11)

משפט: אם אי-רציונלי יש הצגה יחידה שלם משולב אינסופי פשוט.

$$\begin{cases} \alpha_0 = \alpha \\ \alpha_{n+1} = \frac{1}{\alpha_n - [\alpha_n]} \end{cases} \Rightarrow \alpha_n = [\alpha_n] + \frac{1}{\alpha_{n+1}}$$

יציור $d_n = [\alpha_n]$ ונסמן ש- $\alpha = [d_0; d_1, d_2, \dots]$

צריך להראות כמה דברים. ראשית, צריך להראות ש- α_n מוגדר היטב,

סומרי שלמים לא תהיה לנו חלוקה ב-0. זה נכון כי α הוא אי-רציונלי.

מפרט הוא זא שלם. $\Leftrightarrow \alpha_0 - [\alpha_0] \neq 0$ והוא גם אי-רציונלי. $\Leftrightarrow$ וחס α הוא

אי-רציונלי ומפרט לא שלם. ככה ממשיכים באינדוקציה.

$$\alpha = \alpha_0 = d_0 + \frac{1}{\alpha_1} = d_0 + \frac{1}{d_1 + \frac{1}{\alpha_2}} = \dots$$

$$\Rightarrow \alpha = [\alpha_0] = [d_0; \alpha_1] = [d_0; d_1, \alpha_2] = \dots$$

$$\left| \alpha - \frac{p_n}{q_n} \right| = \left| \frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} \right| = \frac{1}{q_{n+1}q_n} = \frac{1}{(\alpha_{n+1}q_n + q_{n-1})q_n} < \frac{1}{q_n^2} \rightarrow 0$$

ראשון p_n ; q_n מורכבים מהשבר הנשאר $[d_0; d_1, \dots, d_n, \alpha_{n+1}]$ והוא הפוך של $[d_0; d_1, \dots, d_n, \alpha_{n+1}]$ וזהו הפוך של α וזהו $\alpha - d_i$

הם שלמים. אכן α_{n+1} איננו יכול להיות ∞ כי אז היינו מקבלים $\alpha = d_i$

חזרה נוכחית וחיבור: $[d_0; d_1, d_2, \dots] = [b_0; b_1, b_2, \dots]$ (זהו) $\alpha = [d_0; d_1, \dots]$

$$d_0 < \alpha < d_0 + 1 \quad \text{אם} \quad \alpha = [d_0; d_1, \dots]$$

$$\Rightarrow d_0 < \alpha < d_0 + 1 \Rightarrow d_0 = \lfloor \alpha \rfloor$$

$$\frac{1}{d_1 + \frac{1}{d_2 + \dots}} = \frac{1}{b_1 + \frac{1}{b_2 + \dots}}$$

$$\Leftarrow b_0 = \lfloor \alpha \rfloor \quad \text{ראשון אופן}$$

$$d_1 + \frac{1}{d_2 + \dots} = b_1 + \frac{1}{b_2 + \dots}$$

$\Leftarrow$ אפשר להמשיך כאילו תהיה α

ובנה באינדוקציה $b_n = d_n \quad \forall n \in \mathbb{N}$

☺

15) 20.11.04
תורה
המשפטים

שיעור זמ ננצח.

תורה על השיעור הקודם:

הזדקנו לזכר משולב פשוט

$$[a_0; a_1, \dots, a_n] = a_0 + \frac{1}{a_1 + \dots + \frac{1}{a_n}}$$

זה זכר סופי... הראנו שלל מספר רציונלי יש הצגה זכר
משולב סופי (ההצגה לא בהכרח יחידה).
למספר אי-רציונלי יש הצגה יחידה זכר משולב אינסופי.

לדוגמה,

$$\frac{56}{20} = 2 + \frac{16}{20} = 2 + \frac{1}{\frac{20}{16}} = 2 + \frac{1}{1 + \frac{4}{16}} = 2 + \frac{1}{1 + \frac{1}{4}}$$

נסמן ב- a_i' את השלמות הנותרות אחרי i שלבים.
קל לראות ש- $a_i' = a_i + \frac{1}{a_{i+1}'}$ זכר
לדוגמה $a_{i-1}' = a_i$ זכר

דוגמה:

(בגלל)

$$a_i' p_{i-1} + p_{i-2} = (a_i + \frac{1}{a_{i+1}'}) p_{i-1} + p_{i-2} =$$

$$= p_i + \frac{p_{i-1}}{a_{i+1}'} = \frac{a_{i+1}' p_i + p_{i-1}}{a_{i+1}'}$$

$$\Rightarrow \frac{a_i' p_{i-1} + p_{i-2}}{a_i' q_{i-1} + q_{i-2}} = \frac{a_{i+1}' p_i + p_{i-1}}{a_{i+1}' q_i + q_{i-1}}$$

לדוגמה

$$(המספר שרוצים לקרב) x = a_0' = a_0 + \frac{1}{a_1'} = \frac{a_1' a_0 + 1}{a_1'}$$

$$\Rightarrow x = \frac{a_i' p_{i-1} + p_{i-2}}{a_i' q_{i-1} + q_{i-2}}$$

פירמה: נניח שרוצים לקרב את $\pi = 3.1415\dots$

התוצר הוא אינסופי ש נראה את השלבים הראשונים.

$$\begin{aligned} \pi &= 3 + 0.1415\dots = 3 + \frac{1}{1/0.1415\dots} = 3 + \frac{1}{7 + 0.065\dots} = 3 + \frac{1}{7 + \frac{1}{1/0.065\dots}} = \\ &= 3 + \frac{1}{7 + \frac{1}{15 + 0.23\dots}} = \dots \end{aligned}$$

המנוגד התק"ל בן $3, 3+\frac{1}{7}, \frac{333}{106}, \dots$
 ברור שיש עוד מספר קירובים - מספר $3, \frac{31}{10}, \frac{314}{100}, \frac{3141}{1000}, \dots$

אנחנו נראה שמחציתם מסוימת - הקירובים בעל-לך שלבים מסודרים הם הכי טובים...

משפט: יהי $x \in \mathbb{R} \setminus \mathbb{Q}$ נתון לפי $x = [a_0; a_1, a_2, \dots]$

אז אם $|x - \frac{p_n}{q_n}| < |x - \frac{p_{n-1}}{q_{n-1}}|$ $n \in \mathbb{N}$

למחלה
$$x - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n(a'_{n+1}q_n + q_{n-1})}$$

הוכחה: פשוט נחשב:

$$\begin{aligned} x - \frac{p_n}{q_n} &= \frac{a'_{n+1}p_n + p_{n-1}}{a'_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} = \frac{q_n(a'_{n+1}p_n + p_{n-1}) + p_n(a'_{n+1}q_n + q_{n-1})}{q_n(a'_{n+1}q_n + q_{n-1})} = \\ &= \frac{q_n p_{n-1} - p_n q_{n-1}}{q_n(a'_{n+1}q_n + q_{n-1})} = \frac{(-1)^n}{q_n(a'_{n+1}q_n + q_{n-1})} \end{aligned}$$

אפשר קודם

⑤

משפט אחר: יהיו $x \in \mathbb{R}$! $\frac{p_n}{q_n}$ בסדר המסלול עבור $n \geq 2$

אז אם $0 < q \leq q_n$ אז $\frac{p}{q} \neq \frac{p_n}{q_n}$ מתקיים $|q_n x - p_n| < |q x - p|$

פשוט, $|x - \frac{p_n}{q_n}| < |x - \frac{p}{q}|$

משמעות: מתוך הרכיבים אם $0 < q \leq q_n$ השבר המשותף נותן

אם הקרוב הכי טוב ל- x .

הוכחה: באמצעות q ו- n .

עבור $n=2$ ההוכחה גושמא בצדדים שישלחו באי-חוליה.

נפרט נסו מקרים:

(I) $q = q_n$ $p \neq p_n$ אז $|\frac{p}{q} - \frac{p_n}{q_n}| \geq \frac{1}{q_n}$ וזהו ל- $p \neq p_n$

באם ל- $n \geq 2$ $|x - \frac{p_n}{q_n}| = \frac{1}{q_n(a'_{n+1}q_n + q_{n-1})} < \frac{1}{2q_n}$

מאידוע השוויון המשותף

$$|x - \frac{p}{q}| \geq |\frac{p}{q} - \frac{p_n}{q_n}| - |x - \frac{p_n}{q_n}| \geq \frac{1}{q_n} - \frac{1}{2q_n} = \frac{1}{2q_n} > |x - \frac{p_n}{q_n}|$$

לפיכך נראה כי $q = q_n$ מתקבל הוכחה.

(II) $q \leq q_{n-1}$ אם הנחת האילוץ צריכה $q < q_n$ אם

↓

$$|q_n x - p_n| = \frac{1}{a'_{n+1} q_n + q_{n-1}}$$

נותר המקרה $p_{n-1} < q < p_n$

תבנית התוכן פתוחה

$$A \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} p \\ q \end{pmatrix}$$

אזכרים $|A| = p_n q_{n-1} - q_n p_{n-1} = (-1)^n \neq 0$ ופיתרון יחיד
(a, b) של המערכת

$$a = \frac{p_{g_{n-1}} - g_{p_{n-1}}}{|A|} = \pm (p_{g_{n-1}} - g_{p_{n-1}}) \in \mathbb{Z}$$

$$b = \frac{p q_n - q p_n}{|A|} = \pm (p q_n - q p_n) \in \mathbb{Z}$$

$$a, b \neq 0 \quad - \text{e} \quad \text{dii}) \quad \frac{p}{q} \neq \frac{p_n}{q_n}, \frac{p_{n-1}}{q_{n-1}} \quad - \text{e} \quad \text{NKD}$$

$g_{n-1} \leq g \leq g_n - 2$, מכאן . הפונקציה f היא $a - b$ וכן,

$f_n a + f_{n-1} b = f_n$, תיבונים אלה סתמים והפוכים:

אם שניכם שלווים וצא ל - 9 שלוו וצא יתן אריות ואם

למרות חיוביים וצא - $q > q_n$ וסדר א ויחיד אחר.

$$ab < 0 \quad \text{gk}$$

אנו חובים מזהרין

$$q_{x-p} = x(q_n a + q_{n-1} b) - (p_n a + p_{n-1} b) =$$

$$= a(q_n X - p_n) + b(q_{n-1} X - p_{n-1})$$

מכיוון $- \frac{p_n}{q_n} \leq \frac{p_{n+1}}{q_{n+1}} \leq x$ מכיוונים שונים נקבע

$$- \mathbb{E} (q_{n+1} X - p_{n+1}) - \delta (q_n X - p_n) \text{ סימנים הפוכים. } \delta$$
$$b(q_n x - p_{n-1}) - a(q_n x - p_n) - d$$

$$\Rightarrow |g^x - p| = |a(q_n x - p_n) + b(q_{n-1} x - p_{n-1})| =$$

$$= |a(q_n x - p_n)| + |b(q_{n-1} x - p_{n-1})| > |a(q_n x - p_n)| \geq |q_n x - p_n|$$



סעיף: והי $x \in \mathbb{R} \setminus \mathbb{Q}$ המקורב "ש" לבר משואה. אזי, $n \in \mathbb{N}$
 מהכרה מתקיים אחד מהשניים:

$$|x - \frac{p_{n+1}}{q_{n+1}}| < \frac{1}{2q_{n+1}^2} \quad \text{או} \quad |x - \frac{p_n}{q_n}| < \frac{1}{2q_n^2}$$

הנחת: מתקיים

$$\frac{1}{q_n q_{n+1}} = \left| \frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} \right| = \left| x - \frac{p_n}{q_n} \right| + \left| x - \frac{p_{n+1}}{q_{n+1}} \right|$$

נניח בשואה ש-

$$|x - \frac{p_{n+1}}{q_{n+1}}| \geq \frac{1}{2q_{n+1}^2} \quad \text{אז} \quad |x - \frac{p_n}{q_n}| \geq \frac{1}{2q_n^2}$$

$$\frac{1}{q_n q_{n+1}} \geq \frac{1}{2q_n^2} + \frac{1}{2q_{n+1}^2} = \frac{q_{n+1}^2 + q_n^2}{2q_n^2 q_{n+1}^2} \quad \text{וכן}$$

$$q_{n+1}^2 + q_n^2 \leq 2q_n q_{n+1}$$

$$(q_{n+1} - q_n)^2 \leq 0$$

$$q_n = q_{n+1}$$

אם נכון

אם נכון

אם נכון

$$q_n = q_{n+1} \quad \text{אז} \quad q_{n+1} = a_{n+1} q_n + q_{n-1}$$

$$n=0 \quad \text{אם} \quad a_{n+1} = 1 \quad \text{אז} \quad q_{n+1} = 0 \quad \text{וזה יתכן לזהות רק אם}$$

$$|x - \frac{p_0}{q_0}| \geq \frac{1}{2} \quad \text{אז כן}$$

$$\frac{p_1}{q_1} - x < p_0 + 1 - x < \frac{1}{2}$$

(11)

סעיף: (המשפט ההפוך) אם $\frac{p}{q}$ רציונלי מצומצם
 אזי $|x - \frac{p}{q}| < \frac{1}{2q^2}$ אזי $\frac{p}{q}$ מופיע בשלם שלם בשאר המשואה
 המקורב x .

הנחת: בהסתמך על משפט איגורס מסיק זריאלי ש $\frac{p}{q}$ שלם
 אזי $|qx - p| \leq |qx - p|$ ו $\frac{p}{q} \neq \frac{p}{q}$ אזי $Q > q$
 $|qx - p| < \frac{1}{2q} \Rightarrow |Qx - p| < \frac{1}{2q} \Rightarrow |x - \frac{p}{Q}| < \frac{1}{2Qq}$

17

דפ

$$\left| \frac{p}{q} - \frac{p}{Q} \right| \leq \left| x - \frac{p}{q} \right| + \left| x - \frac{p}{Q} \right| < \frac{1}{2q^2} + \frac{1}{2qQ}$$

דפ $\left| \frac{p}{q} - \frac{p}{Q} \right| \geq \frac{1}{qQ}$ וקטל $\frac{p}{Q} \neq \frac{p}{q}$ - נאמר ש-

$$\frac{1}{qQ} < \frac{1}{2q^2} + \frac{1}{2qQ} = \frac{q+Q}{2q^2Q}$$

$$(*) \cdot Q > q \quad \Leftarrow \quad q + Q > 2q \quad \Leftarrow$$

דפ, נאמר התנאי הזה אכן חזר אלא שצריך ?

נניח ש- $\frac{p}{q}$ דפ בסדר הנשוא. אזי $q_{n+1} < q < q_n$
 אולם ראוי ש- $|qx-p| = |a(q_n x - p)| + |b(q_{n+1} x - p_{n+1})|$
 וזה גורל נ- $|q_{n+1} x - p_{n+1}|$ דפ $Q = q_{n+1}$ סתרי א- (*)

☺

ניתן לזכור את החסם .

טענה: (לא הוכח) ובי $x \in \mathbb{R} \setminus \mathbb{Q}$ המקרה "לבר משלב.
 אזי לפחות אחת מבין $\frac{1}{q}$ שלם מנוח חזק יותר
 כצפוי מקי"מ $\left| x - \frac{p_n}{q_n} \right| < \frac{1}{\sqrt{5} q_n^2}$
 ככה מקימים לחסם של משלב הורוביץ.

דוגמה: קצ"כ בהנחה לבר משלב אי אפשר לדעת מה
 המספר לפני מ"צ. אבל יש מקרים לבהם זה אולי.
 דוגמה $x = 1 + \frac{1}{x}$ אז $x = 1 + \frac{1}{1 + \frac{1}{1 + \dots}}$

המשוואה הזאת אפשר לפתור ...

לברורים מתמטיים מחזוריים

תלכודת:

$$① \quad p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$$

$$② \quad \alpha_n = \lfloor \alpha_n \rfloor + \frac{1}{\alpha_{n+1}} = a_n + \frac{1}{\alpha_{n+1}}$$

$$\alpha_0 = \alpha$$

$$③ \quad \alpha = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}}$$

$$④ \quad \alpha - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n (\alpha_{n+1} q_n + q_{n+1})}$$

סדרת פיבונצ'י: 0, 1, 1, 2, 3, 5, 8, ...

צומח

$$F_0 = 0$$

$$F_1 = 1$$

$$F_n = F_{n-1} + F_{n-2}$$

נסתם על השבר המסלול $\alpha = [1, 1, 1, \dots]$ מתקיים

$$p_{-1} = 1 \quad p_0 = 1$$

$$p_n = F_{n+1}$$

$$q_n = F_n$$

$$\alpha^2 - \alpha - 1 = 0 \quad \alpha = \alpha_0 = a_0 + \frac{1}{\alpha_1} = 1 + \frac{1}{\alpha}$$

$$\phi = \frac{\sqrt{5}+1}{2}$$

$$\phi^{-1} = \frac{\sqrt{5}-1}{2}$$

$$F_{n+1} F_{n-1} - F_n^2 = (-1)^n$$

נשים לב שמתקיים

$$F_n = \frac{1}{\sqrt{5}} (\phi^n - (-\frac{1}{\phi})^n) \quad \text{משפט 1.5}$$

$$0 = F_0 = \frac{1}{\sqrt{5}} (\phi^0 - (-\frac{1}{\phi})^0)$$

$$1 = F_1 = \frac{1}{\sqrt{5}} (\frac{\sqrt{5}+1}{2} + \frac{\sqrt{5}-1}{2})$$

נניח שמתקיים $n-1$ ו- $n-2$ ונניח

$$F_n = F_{n-1} + F_{n-2} = \frac{1}{\sqrt{5}} (\phi^{n-1} - (-\frac{1}{\phi})^{n-1}) + \frac{1}{\sqrt{5}} (\phi^{n-2} - (-\frac{1}{\phi})^{n-2}) =$$

$$= \frac{1}{\sqrt{5}} (\phi^{n-2}(\phi-1) - (-\frac{1}{\phi})^{n-2}(-\frac{1}{\phi}+1)) = \frac{1}{\sqrt{5}} (\phi^n - (-\frac{1}{\phi})^n)$$

⑤

דוגמה: (היה לקרב את $\sqrt{2}$ מתחילים) $a_0 = 1$ ניקח

$$\sqrt{2} - 1 = \frac{1}{\sqrt{2} - 1} = \frac{1}{\frac{1}{\sqrt{2} - 1} \cdot \frac{\sqrt{2} + 1}{\sqrt{2} + 1}} = \frac{1}{\frac{\sqrt{2} + 1}{2 - 1}} = \frac{1}{\sqrt{2} + 1} = \frac{1}{2 + \sqrt{2} - 1}$$

למה זה להתחיל מתחילי?
אז הפסגה של $\sqrt{2}$ יהיה מתחילי

הגדרה: (אחר שלבר משותף $\alpha = [a_0, a_1, \dots]$ הוא מתחילי אם קיימים $r \in \mathbb{N}$ וק של $n > r$ $a_{n+1} = a_n$

המקרה זה מסומנים: $\alpha = [a_0, \dots, a_r, a_{r+1}, \dots, a_{r+e}]$

(אחר שלבר הוא מתחילי פסגה אם המתחילי מתחילי ב- a_0

מספר אירציונלי α נקרא ריכוזי אם קיים פולינום P ממונה
ג רק ש- $P(\alpha) = 0$ ואין פולינום P' ממונה (מנוה יתר) רק
ש- $P'(\alpha) = 0$ (הפולינומים המקדמים רציונליים)

משפט לגרנצ' (2) מספר $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ הוא ריכוזי אם

השבר המשותף שלו מתחילי.

הוכחה:

(נתח) מהמקרה הפרטי ש- $\alpha = [a_0, a_1, \dots, a_{l-1}]$ בעל

$$\alpha = \frac{a_{l-1}p_{l-1} + p_{l-2}}{a_{l-1}q_{l-1} + q_{l-2}} \iff \alpha_l = \alpha$$

$$\alpha^2 q_{l-1}^2 + \alpha (q_{l-2} p_{l-1} - p_{l-2} q_{l-1}) - p_{l-2}^2 = 0 \iff$$

אז α שורש של פולינום המקדמים שלמים $\iff \alpha$ ריכוזי.

המקרה הכללי, יהי $\beta = [b_0, b_1, \dots, b_r, b_{r+1}, \dots, b_{r+e}]$ (סו)

$\alpha = [b_{r+1}, \dots, b_{r+e}]$ סומר, $\beta = [b_0, b_1, \dots, b_r, \alpha]$ סכ

$$(*) \quad \beta = \frac{\alpha \cdot p_r + p_{r-1}}{\alpha \cdot q_r + q_{r-1}}$$

לפי המקרה הפרטי קיימים $A, B, C \in \mathbb{Q}$ וק ש- $A\alpha^2 + B\alpha + C = 0$

נחשב $A', B', C' \in \mathbb{Q}$ וק ש- $A'\beta^2 + B'\beta + C' = 0$ (**) $A' = A$

אתי הצבר, (*), ב- (***) וצמצומים ופירוחים פולינומים מתקדם

$\triangleleft$ יש מספר סופי של A_n, B_n, C_n שסכומם α אינו
 יש אינסוף חזרים, אם יש שלוש שלמות A, B, C
 לפחות 3 פאסים, ונניח עבור $\alpha_1, \alpha_2, \alpha_3$ אז שלוש
 מספרים אלה פתורים באינסוף משוואות שלמות, אם הוכחה
 שניים מהם שלמים (אם $\alpha_1 = \alpha_2$). $\triangleleft$ α ממוזג!! $\odot$

הצדקה:

יהי α אירציונלי. רחוקי הצדקה של α הוא השורש הנסי של
 הפולינום המניחה של α . אם $\alpha = \frac{a+b\sqrt{d}}{c}$ ואז
 $a, b, c, d \in \mathbb{Z}$, d חופשי מקוברים אז $\alpha' = \frac{a-b\sqrt{d}}{c}$
 α נקרא ממוזג אם $\alpha > 1$ או $0 < \alpha' < 1$.
 (למשל $1 + \sqrt{2}$ הוא ממוזג)

משפט 3: נשבר השורש של α הוא ממוזג. אם
 אחר α ממוזג, למקרה כזה אם $\alpha = [a_0, \dots, a_n]$
 אז $\alpha' = [\overline{a_n}, \dots, \overline{a_0}] = \frac{1}{\alpha}$

היותו קדם לראות ש- $(\alpha + \beta)' = \alpha' + \beta'$ ו- $(\alpha\beta)' = \alpha'\beta'$.
 ומאחר $1' = 1$ ו- $(\frac{1}{\alpha})' = \frac{1}{\alpha'}$ נקבע כי
 נניח $\alpha = a_n + \frac{1}{\alpha_{n+1}}$ (הוא ממוזג) אם כי

$\triangleleft \alpha' = a_n + \frac{1}{\alpha'_{n+1}}$ נראה באינדוקציה על α
 ממוזג אז α ממוזג. מסיום באינדוקציה נכון
 כי $\alpha_0 = \alpha$ נניח על α_n ממוזג אז

$\alpha_n > 1$ או $0 < \alpha'_n < 1$.
 $\triangleleft \frac{1}{\alpha'_{n+1}} < -1 \triangleleft a_n \geq 1$, $0 > a_n + \frac{1}{\alpha'_{n+1}}$
 $\triangleleft \alpha_{n+1} \geq 1$ ו- $\alpha_{n+1}' = \frac{1}{\alpha_n' - a_n} \leq 0$

$\triangleleft$ באינדוקציה נניח כי α_n ממוזג.
 $\alpha_n' = a_n + \frac{1}{\alpha'_{n+1}}$ ו- $0 < \alpha_n' < 1$
 $a_n = \lfloor \alpha_n \rfloor = \lfloor L - \frac{1}{\alpha_{n+1}} \rfloor$

(20)

α אורציונלי ריבועי, אז α שטח מתצוי $\Leftarrow$ קיימים

$$a_k = a_m \Leftarrow \alpha_k = \alpha_m \quad k < m$$

$$a_{k+1} = \left\lfloor -\frac{1}{\alpha'_k} \right\rfloor = \left\lfloor -\frac{1}{\alpha'_m} \right\rfloor = a_{m-1}$$

$\Leftarrow \alpha_{k-1} = \alpha_{m-1}$ המשך האינדוקציה ונקטת α מתצוי דלמארו.

מצד שני, נניח $\alpha = [a_0, \dots, a_{l-1}]$ ונראה שהוא מצומצם.

$$\alpha = \frac{\alpha p_{l-1} + p_{l-2}}{\alpha q_{l-1} + q_{l-2}} \quad \alpha_l = \alpha$$

$\Leftarrow \alpha$ שטח של הפולינום $p(x) = q_{l-1}x^2 + (q_{l-2} - p_{l-1})x - p_{l-2}$
 $\alpha > 1$ כי $a_0 = a_l \geq 1$ (ממשונות)

צריך להראות $-1 < \alpha' < 0$ אבל α' הוא השורש

השני של $p(x)$. נשים לב $p(0) = -p_{l-2} < 0$ ו

$$p(-1) = q_{l-1} - q_{l-2} + p_{l-1} - p_{l-2} =$$

$$= (a_{l-1} q_{l-2} + q_{l-3}) - q_{l-2} + (a_{l-1} p_{l-2} + p_{l-3}) - p_{l-2} =$$

$$= (a_{l-1} - 1)(q_{l-2} + p_{l-2}) + q_{l-3} + p_{l-3} > 0$$

$\Leftarrow$ ממעט אז הביניים קיימים $p(x)$ שורש α' בין 0 ל -1 .

נניח α מתצוי $\Leftarrow$ המשך ההוכחה.

$$\alpha = [a_0, a_1, \dots, a_{l-1}] \quad \alpha_k$$

$$\alpha' = \alpha'_0 = a_0 + \frac{1}{\alpha'_1}, \quad \alpha'_1 = a_1 + \frac{1}{\alpha'_2}, \quad \dots, \quad \alpha'_{l-1} = a_{l-1} + \frac{1}{\alpha'_l}$$

$$-\frac{1}{\alpha'_1} = a_0 - \alpha'_0, \quad \dots, \quad -\frac{1}{\alpha'_{l-1}} = a_{l-2} - \alpha'_{l-2}, \quad -\frac{1}{\alpha'_l} = a_{l-1} - \alpha'_{l-1}$$

$$-\frac{1}{\alpha'_l} = a_{l-1} - \alpha'_{l-1} = a_{l-1} + \frac{1}{-\frac{1}{\alpha'_{l-2}}} = a_{l-1} + \frac{1}{a_{l-2} - \alpha'_{l-2}}$$

וככה אפשר להמשיך והשגת α'_{l-2} וקטן מהמשוואה

$$-\frac{1}{\alpha'_l} = [a_{l-1}, a_{l-2}, \dots, a_0]$$

(21)

② 4/12/07
תאריך
המספרים

שיעור 8 סיני

צדקה:
יהי

$d \in \mathbb{N}$ יק, $\sqrt{d} \notin \mathbb{N}$ אז

$$\star \sqrt{d} = [\sqrt{d}, a_1, a_2, \dots, a_2, a_1, 2\sqrt{d}]$$

ראש x הוא הערך השלם של x .

* הטענה ההפוכה גם נכונה במידה מסוימת. אם יש
למר מהצורה $\star$ אז הוא שווה של מספר רציונלי (אז)
בזקא טבעי).

הנחה: (סמ) $\alpha = \sqrt{d} + \sqrt{d}$! $\alpha' = \sqrt{d} - \sqrt{d}$

מתקיים $0 < \alpha' < 1$; $1 < \alpha$. עק השני המשוב של α
הוא מסווגי למסווגי ומתקיים

$$-\frac{1}{\alpha'} = [\overline{a_{i-1}, \dots, a_i, a_0}] \quad \alpha = [\overline{a_0, \dots, a_{i-1}}]$$

$$\sqrt{d} + \sqrt{d} = [\overline{2\sqrt{d}, a_1, \dots, a_{i-1}}] = [\overline{2\sqrt{d}, a_1, \dots, a_{i-1}, 2\sqrt{d}}]$$

$$\Rightarrow \sqrt{d} = [\sqrt{d}, a_1, \dots, a_{i-1}, 2\sqrt{d}]$$

מצד שני,

$$\sqrt{d} = \sqrt{d} + \sqrt{d} - \sqrt{d} = \sqrt{d} + \frac{1}{\frac{1}{\sqrt{d}} - \sqrt{d}} = [\sqrt{d}, -\frac{1}{\alpha'}]$$

אז

$$-\frac{1}{\alpha'} = [\overline{a_{i-1}, \dots, a_i, 2\sqrt{d}}] = \sqrt{d} - \sqrt{d}$$

$$\Rightarrow \sqrt{d} = [\sqrt{d}, a_{i-1}, \dots, a_i, 2\sqrt{d}]$$

ראש $a_i = a_{i-1}$ וזה בדיוק מה שרצינו.

③

(סמ) $G = SL_2(\mathbb{Z})$ קבוצת המטריצות ההפיכות

מ $\mathbb{Z}$, שומר את המטריצה $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ כאשר $a, b, c, d \in \mathbb{Z}$

$$ad - bc = \pm 1$$

הערך בעולה של המטריצה α מסומן

אם $\alpha \in \mathbb{R}$! $\sigma \in G$ גזיר

$$\sigma \alpha = \frac{a\alpha + b}{c\alpha + d}$$

$(\sigma\tau)\alpha = \sigma(\tau\alpha)$ כש $\alpha \in \mathbb{R}$; $\sigma, \tau \in G$ כש
 (חישוב פשוט) ונגזיר $\alpha \sim \beta$ כאשר קיים $\sigma \in G$ כך
 ש- $\sigma\alpha = \beta$, לכן אפשר לקיים $a, b, c, d \in \mathbb{Z}$ כך ש-

$$\frac{a\beta + b}{c\beta + d} = \alpha \quad \text{כש} \quad ad - bc = \pm 1$$

קדם הראוי לנו יחס שקילות.

לענין: במוסכמה הרצונית של קווים זה לזה.
הוכחה: מספיק להראות של הרצונית של קווים $0 \neq 1$.
 ניקח $\alpha = \frac{p}{q}$ כש $\alpha = \frac{a \cdot 0 + p}{c \cdot 0 + q}$.
 נגדל p ו- q זרים כש $aq - pc = 1$ (הא-גורמים של אוילר)
 יש a, b כך ש- $aq - pc = 1$. $\alpha \sim 0 \iff$
 וזהו מהסנטיסיביות של β ו- α (רצונית) $\alpha \sim \beta$. (ii)

לענין: יפוי $\alpha \in \mathbb{R} \setminus \mathbb{Q} = [a_0, a_1, \dots, a_n, \dots]$ כש $\alpha \sim a_n$
 שם $n \in \mathbb{N}$ נאמר $a_n = [a_n, a_{n+1}, \dots]$
הוכחה: יפוי ל-

$$\alpha = [a_0, \dots, a_{n-1}, a_n] = \frac{p_{n-1}\alpha_n + p_{n-2}}{q_{n-1}\alpha_n + q_{n-2}}$$

נאמר $p_{n-1}, p_{n-2}, q_{n-1}, q_{n-2} \in \mathbb{Z}$, $p_{n-1}q_{n-2} - p_{n-2}q_{n-1} = \pm 1$,
 כש $\alpha = \sigma a_n$ נאמר

$$\sigma = \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix}$$

(ii) . $\alpha \sim a_n \iff \sigma \in G \iff |\sigma| = \pm 1$!

לענין: $|A_n| = -1$ כש $A_n = \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix}$, $|A_0|$

$A_0 A_1 \dots A_n = \sigma_{n-1}$ כש σ_{n-1}^{-1} מהסנטיביות הקודמת.

$$A_n \alpha_{n-1} = \frac{A_n \alpha_{n-1} + 1}{\alpha_{n-1}} = a_n + \frac{1}{\alpha_{n-1}} = \alpha_n \quad \text{הוכחה:}$$

$$\Rightarrow A_0 A_1 \dots A_n \alpha = \alpha_n = \sigma_{n-1} \alpha$$

(ii)

22

מהו המ"צ של 0? אנתנו צרכים לנ"ל

$$\text{אם } ad-bc=1 \text{ אז } a,b,c,d \in \mathbb{Z}$$

$$0 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} 0 = \frac{a \cdot 0 + b}{c \cdot 0 + d} = \frac{b}{d}$$

$$a, d = \pm 1 \iff ad = 1 \iff b = 0 \iff$$

c נקבע באופן שרירותי. אז המ"צ הם

$$\left\{ \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ c & -1 \end{pmatrix} : c \in \mathbb{Z} \right\}$$

מה המ"צ של α בל"ל?

צרכים לנ"ל $ad-bc=1$ אז $a,b,c,d \in \mathbb{Z}$

$$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \alpha = \frac{a\alpha + b}{c\alpha + d}$$

$$\Rightarrow c\alpha^2 + (d-a)\alpha - b = 0$$

אם $c=0$ אז $a \neq d$ אז α רציונלי.

אם $c \neq 0$ אז α אי-רציונלי.

אז המ"צ הם לא טריוויאלי רק אם α הוא רציונלי או אי-רציונלי.

אם $\alpha \sim \beta$ אז $\alpha \sim \beta$ קיים m, n כך $\alpha_n = \beta_m$ Secret על

האותה:

$$\alpha \sim \beta \iff \alpha \sim \alpha_n = \beta_m \sim \beta \quad (\Rightarrow)$$

$$\alpha = \sigma \beta = \frac{a\beta + b}{c\beta + d} \quad ; \quad \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \quad \text{על} \quad (\Leftarrow)$$

לפי: אם $\beta > 1$ אז $c > d > 0$ אז $\frac{a}{c} > \frac{b}{d}$ אז $\frac{a}{c}$ רציונלי

אז $\beta = \frac{a}{c}$ חלקי חלקי חסומה

האותה: $(a, c) = 1$ אז $ad-bc = \pm 1$ אז $\frac{a}{c}$ רציונלי

משלב סופי:

$$\frac{a}{n} = [a_0, \dots, a_{n-1}] = \frac{p_{n-1}}{q_{n-1}} = \frac{a}{c}$$

$$(*) \quad p_{n-1}q_{n-2} - q_{n-1}p_{n-2} = (-1)^n$$

$$ad-bc = (*) \quad \text{על} \quad n \text{ זוגי}$$

$$\Rightarrow ad-bc = p_{n-1}d - q_{n-1}b$$

$$p_{n-1}q_{n-2} - q_{n-1}p_{n-2} = ad - bc = p_{n-1}d - q_{n-1}b$$

$$p_{n-1}(d - q_{n-2}) = q_{n-1}(b - p_{n-2})$$

$$(q_{n-1}, p_{n-1}) = 1$$

$$\Rightarrow q_{n-1} \nmid p_{n-1}, \quad q_{n-1} \mid (d - q_{n-2})$$

$$q_{n-2} \leq q_{n-1} \quad q_n \text{ לא חייב להיות!} \quad d < q_{n-1} = c \quad \text{ההפך}$$

$$\Rightarrow |d - q_{n-2}| < q_{n-1}$$

$$\Rightarrow d - q_{n-2} = 0 \Rightarrow d = q_{n-2}$$

$$\text{כאן כאן} \quad b - p_{n-2} = 0 \Rightarrow b = p_{n-2}$$

$$\Rightarrow \alpha = \frac{p_{n-1}\beta + p_{n-2}}{q_{n-1}\beta + q_{n-2}}$$

$$\Rightarrow \alpha = [a_0, \dots, a_n, \beta]$$

המשפט הנ"ל

$$c\alpha + b > 0 \quad \text{כאן} \quad \beta = \sigma\alpha = \frac{a\alpha + b}{c\alpha + d} \quad ; \quad \alpha \sim \beta \quad \text{כאן}$$

זכור: $(-\sigma \text{ לא בסדר})$

$$\alpha = \sigma_{n-1} \alpha_n \quad \sigma_{n-1} = \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix}$$

$$\beta = \sigma \sigma_{n-1} \alpha_n$$

$$\sigma \sigma_{n-1} = \begin{pmatrix} * & * \\ c p_{n-1} + d q_{n-1} & c p_{n-2} + d q_{n-2} \end{pmatrix} = \sigma' \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$$

$$c' = c p_{n-1} + d q_{n-1} = q_{n-1} \left(c \frac{p_{n-1}}{q_{n-1}} + d \right)$$

$$d' = c p_{n-2} + d q_{n-2} = q_{n-2} \left(c \frac{p_{n-2}}{q_{n-2}} + d \right)$$

$$c \frac{p_n}{q_n} + d > 0 \quad \text{כל } n \quad \Leftrightarrow \frac{p_n}{q_n} \rightarrow \alpha$$

$$\text{כל } n \quad 0 < c', d' \quad \Leftrightarrow 0 < \frac{p_n}{q_n}$$

$$\alpha_n = \beta_m \quad \text{כל } n, m \quad \Leftrightarrow c' > d' \quad \Leftrightarrow \frac{p_{n-1}}{q_{n-1}} > \frac{p_{n-2}}{q_{n-2}}$$

(11)

כל $n, m \in \mathbb{N}$

(22)

נושאים לסור הקורס

- 1) תאורטיקה של חסמים (נק' שיג' בתופים קלאסים)
(2 שיעורים) תנ"כ, סנ'
 - 2) מספרים אלגבריים / טרנסצנדנטים (משפט עיוכרל, חספכיים π , e) (2 שיעורים) נוע', כור
 - 3) מבוא למשפט נור (ניסח המשפט + אפליקציות
עמנואל ציופנסיו) נועם
 - 4) מבוא ל- abc (ניסוח ומסקנה) צוק (15)
 - 5) אינדוקציה של $\sum \frac{1}{n^3}$ (בלחה) אליאב
 - 6) משפט נור (בלחה) (2 שיעורים)
- היכנתים: ה- 18/12 יהיה שיעור א-ה 9-13

משוואת פל

ב הספור התחיל לפני המון שנים בשארכימדיס שלח חיידה
(שהוא כנראה בעצמו) לא ידע לפתור) לחיידים של ארכימדיס
רק בשנת 1896 הצליחו למצוא פיתרון אחד לחיידה...

היידה: משוואת מהצורה $x^2 - dy^2 = 1$ נקראת משוואת פל

למשוואה יש פיתרון טריוויאלי - $x = \pm 1$; $y = 0$
(אנחנו מתעלים רק פתרונות שלמים).

אז אנחנו לוקחים את המשוואה הזו ו- d ריבועי,
כלומר $d = n^2$ אז $(x + yn)(x - yn) = x^2 - dy^2 = 1$
 $x + yn$; $x - yn$ צריכים להיות שווים סימן.

$$2x = (x + yn) + (x - yn) = \pm 2 \quad \Leftarrow$$

$$\left\{ \begin{array}{l} x = \pm 1 \\ y = 0 \end{array} \right. \quad \Leftarrow \text{להפיתרון הטריוויאלי אז זה לא מעניין, ואנחנו לוקחים את ה- } d \text{ לא ריבועי.}$$

נשים לב ש- (x, y) פיתרון אז $(\pm x, \pm y)$ פתרונות.

היידה: פיתרון (x, y) למשוואת פל יקרא חיוכי אם $x, y \geq 0$

משפט 1: אם (p, q) פיתרון ^{חיוכי} למשוואת פל $x^2 - dy^2 = 1$ אז

p, q חלקי של השלם המשותף המ"צ, או $\sqrt{d}$

הוכחה: (p, q) פיתרון $\Leftarrow p^2 - dq^2 = 1$

$$(p - q\sqrt{d})(p + q\sqrt{d}) = 1 \quad \Leftarrow$$

$$\frac{p}{q} - \sqrt{d} = \frac{1}{q(p + q\sqrt{d})} > 0 \quad \Leftarrow$$

$$p > q\sqrt{d} \quad \Leftarrow$$

$$0 < \frac{p}{q} - \sqrt{d} = \frac{1}{q(p + q\sqrt{d})} < \frac{\sqrt{d}}{q(q\sqrt{d} + q\sqrt{d})} = \frac{1}{2q^2}$$

אפי משה שראינו בשיעור קודם זה גורם $\frac{p}{q}$ - ל- $\frac{p}{q}$ היא מנה
חלקיה בפיתול של $\sqrt{d}$
(11)

הזרה: המספר הזה לא ניתן בכיוון ההפוך. כלומר מנה חלקיה
מקיימת את משוואת פא. למשל $\frac{4}{3}$ מופיע בפיתול של $\sqrt{2}$
אבל $4^2 - 3^2 \cdot 2 \neq 1$

אנחנו יודעים $[a_0; a_1, \dots]$ הפיתול של $\sqrt{d}$ כלומר מסתבר
אינסופי. נגדור s_k, t_k באופן הבא:

$$s_0 = 0 \quad t_0 = 1$$

$$s_{k+1} = a_{k+1} t_k - s_k \quad t_{k+1} = \frac{d - s_{k+1}^2}{t_k}$$

אז

(12) s_k, t_k מספרים שלמים $t_k \neq 0$

(13) $t_k \mid (d - s_k^2)$

(14) $\alpha_k = \frac{s_k + \sqrt{d}}{t_k}$ (השארית של הפיתול)

הוכחה: האינדוקציה על k .

עבור $k=0$ האזכאי $s_0, t_0 \in \mathbb{Z}$; $t_0 = 1 \neq 0$ כמו כן,
 $d - s_0^2 = d$; $t_0 = 1$ ואכן $1 \mid d$.
וכן $\alpha_0 = \frac{s_0 + \sqrt{d}}{t_0} = \sqrt{d}$

נניח כעת שהסדרה $k-1$ (נכונה) - s_{k+1}, t_{k+1} .

(15) $s_{k+1} = a_{k+1} t_k - s_k \in \mathbb{Z}$ שלמים s_k, t_k, a_k

אם $t_{k+1} = 0$ אז $d = s_{k+1}^2$ וסיימנו לוק $d = 0$

אם ריבועי.

$$t_{k+1} = \frac{d - s_{k+1}^2}{t_k} = \frac{d - s_k^2}{t_k} + 2a_{k+1}s_k - a_{k+1}^2 t_k \in \mathbb{Z}$$

לפי

הנחת האינדוקציה

(16) $t_{k+1} \mid (d - s_{k+1}^2) \iff t_k \cdot t_{k+1} = d - s_{k+1}^2$

(17) $\alpha_{k+1} = \frac{1}{\alpha_k - a_{k+1}} = \frac{t_k}{(s_k + \sqrt{d}) - t_k a_{k+1}} = \frac{t_k}{\sqrt{d} - s_{k+1}} = \frac{t_k (s_{k+1} + \sqrt{d})}{d - s_{k+1}^2} = \frac{s_{k+1} + \sqrt{d}}{t_{k+1}}$

(11)

(25)

הצגה של $\frac{p_k}{q_k}$ היא הנדסה והתקן הסתם $\mathbb{Q}$
 $\sqrt{d}$ אינו מסומן $k \geq 0$ מתקיים
 $p_k^2 - d q_k^2 = (-1)^{k+1} \cdot t_{k+1}$

$$t_{k+1} > 0$$

הוכחה: $\sqrt{d} = [a_0; a_1, a_2, \dots, a_k, \alpha_{k+1}]$ וכן

$$\sqrt{d} = \frac{\alpha_{k+1} p_k + p_{k-1}}{\alpha_{k+1} q_k + q_{k-1}}$$

$$\alpha_k = \frac{s_{k+1} + \sqrt{d}}{t_{k+1}} \quad \text{כאשר}$$

$$\Rightarrow \sqrt{d} = \frac{(s_{k+1} + \sqrt{d}) p_k + p_{k-1} t_{k+1}}{(s_{k+1} + \sqrt{d}) q_k + q_{k-1} t_{k+1}}$$

$$\Rightarrow \underbrace{\sqrt{d} (s_{k+1} q_k + t_{k+1} q_{k-1} - p_k)}_{\in \mathbb{Q}} = \underbrace{s_{k+1} p_k + t_{k+1} p_{k-1} - d q_k}_{\in \mathbb{Q}}$$

האיברים הנציינ'ים צריכים להיות שווים

$$(1) \quad s_{k+1} q_k + t_{k+1} q_{k-1} = p_k \quad / \cdot p_k$$

$$(2) \quad s_{k+1} p_k + t_{k+1} p_{k-1} = d q_k \quad / \cdot - q_k$$

$$\Rightarrow p_k^2 - d q_k^2 = t_{k+1} (p_k q_{k-1} - p_{k-1} q_k) = (-1)^{k+1} t_{k+1}$$

מתקיים $t_{k+1} > 0$ וכן $k \geq 0$ מתקיים

$$\frac{p_{2k}}{q_{2k}} = C_{2k} < \sqrt{d} < C_{2k+1} = \frac{p_{2k+1}}{q_{2k+1}}$$

$$p_k^2 - d q_k^2 < 0 \quad \text{אם } k \text{ זוגי}$$

$$p_k^2 - d q_k^2 > 0 \quad \text{אם } k \text{ אי-זוגי}$$

וזהו מה שרצינו $p_k^2 - d q_k^2 = (-1)^{k+1} t_{k+1}$ וכן $t_{k+1} > 0$

☺

מסקנה: אם n הוא אי-זוגי, אז $\sqrt{d}$ אינו מסומן
 אם n זוגי, אז $\sqrt{d}$ מסומן

הוכחה: $\Rightarrow$ $\sqrt{d} = [a_0; \overline{a_1 \dots a_n}]$ וזוהי - j מספר קיים k
 יק - e $n_k = j$ $\alpha_{k+1} = \alpha_1$ (כאן הוספתי)
 סעיף 180 (ג) מכאן, נרשם

$$\frac{S_{k+1} + \sqrt{d}}{t_{k+1}} = \frac{S_1 + \sqrt{d}}{t_1}$$

$$\Rightarrow \underbrace{\sqrt{d}}_{\notin \mathbb{Q}} \underbrace{(t_{k+1} - t_1)}_{\in \mathbb{Q}} = \underbrace{S_{k+1} t_1 - S_1 t_{k+1}}_{\in \mathbb{Q}}$$

$$\Rightarrow t_{k_{n+1}} = t_1, \quad s_{k_{n+1}} = s_1$$

$$\Rightarrow t_i = d - s_i^2 = d - S_{kn+1}^2 = t_{kn} t_{kn+1} = t_{kn} t_1$$

$$\Rightarrow t_{kn} = 1$$

[illegible]

$$[\alpha_j] = s_j + [\sqrt{d}] = s_j + a_0 \triangleq \alpha_j = s_j + \sqrt{d} \quad d \in \mathbb{N}$$

$$\Rightarrow \alpha_j = [\alpha_j] + \frac{1}{\alpha_{j+1}} = s_j + a_0 + \frac{1}{\alpha_{j+1}}$$

$\rho_{NN}^{\text{eff}} \quad \rho_{\text{eff}} \quad t_0 = 1 \quad -0.81$

$$a_0 + \frac{1}{\alpha_1} = \alpha_0 = \sqrt{d} = \alpha_j - s_j = a_0 + \frac{1}{\alpha_{j+1}}$$

$$\Rightarrow \alpha_i = \alpha_j + 1$$

אז הסדרה גם מחזירה - $j \leq j|n$. 

משפט 2: יהיו $\frac{p_k}{q_k}$ הרציונל החלקי-גדול בעייתיות של $\sqrt{d}$ ושל α מסוג. יהיו n אורך המחזור של השבר. אז

10. $x^2 - dy^2 = 1$ (2 ס"ס) ח"ח. הסתמך ב-15.4.5 n ס"ס (10)

$$X = p_{kn-1} \quad Y = q_{kn-1} \quad k = 1, 2, 3, \dots$$

(ב) אם n איננו 6 הפתרונות היחידים של $x^2 - dy^2 = 1$ הם

$$x = p_{kn-1} \quad y = q_{kn-1} \quad k=2, 4, 6, \dots$$

26

הוכחה: ראוי של פיתרון (x_0, y_0) הוא מנה חלקי

(p_j, q_j) עבור j כלשהו. לפי טענה העולה נובע ש-

$$p_j^2 - d q_j^2 = (-1)^{j+1} t_{j+1}$$

$\Leftarrow (p_j, q_j)$ פיתרון אמיתי $j+1$ הוא $t_{j+1} = 1$

אם $j+1 = nk \Leftarrow j+1 \nmid n \Leftarrow t_{j+1} = 1$ מה נצטרך להוכיח?

אם n הוא אי-זוגי אם $j+1$ הוא אי-זוגי אם n אי-זוגי אם

$j+1$ הוא זוגי רק -1 או 1 הוא אי-זוגי או 1 .

ii)

הערה: בהנחת משוואת פיתרון (x, y) נאמר ש-

הוא הפיתרון החיובי הקטן ביותר, כלומר פיתרון חיובי אחר

(x', y') מתקיים $x < x'$ (זה גם גורם $y < y'$).

משפט 3: יהי (x_1, y_1) פיתרון (בסיסי) למשוואה $x^2 - dy^2 = 1$. אז

כל זוג מספרים שלמים x_n, y_n המקיימים

$$x_n + \sqrt{d} y_n = (x_1 + \sqrt{d} y_1)^n$$

הם פיתרון למשוואה.

הוכחה: נשים לב ש- $x_n - y_n \sqrt{d} = (x_1 - y_1 \sqrt{d})^n$ גם זה נכון.

ההערה: $a + b\sqrt{d} \mapsto a - b\sqrt{d}$ היא אוטומוर्फיסם של $\mathbb{Q}(\sqrt{d})$.

$$\sigma(xy) = \sigma(x) \sigma(y)$$

$$\sigma(x+y) = \sigma(x) + \sigma(y)$$

$$\Rightarrow x_n - \sqrt{d} y_n = \sigma(x_n + \sqrt{d} y_n) = \sigma((x_1 + \sqrt{d} y_1)^n) = (\sigma(x_1 + \sqrt{d} y_1))^n = (x_1 - \sqrt{d} y_1)^n$$

כך,

$$x_n^2 - dy_n^2 = (x_n + y_n \sqrt{d})(x_n - y_n \sqrt{d}) = (x_1 + y_1 \sqrt{d})^n (x_1 - y_1 \sqrt{d})^n = (x_1^2 - dy_1^2)^n = 1^n = 1$$

(x_n, y_n) פיתרון $\Leftarrow$

iii)

משפט 4: יהי (x, y) פיתרון בסדר ראשון של $x^2 - dy^2 = 1$. אז (x_n, y_n) פיתרון
 תיכני של המשוואה הוא מהצורה (x_n, y_n) כאשר (x_1, y_1) (קבוצת $\mathbb{Z}$)

$$x_n + y_n \sqrt{d} = (x_1 + y_1 \sqrt{d})^n$$

הוכחה: נניח בראשונה שקיים פיתרון (u, v) של אינו מתקבל הצורה הנדרשת.

נשים לב ש- $x_1 + y_1 \sqrt{d} > 1$ אז $(x_1 + y_1 \sqrt{d})^n \rightarrow \infty$ כאשר n גדל.
 נקבל $(x_1 + y_1 \sqrt{d})^n < u + v \sqrt{d} < (x_1 + y_1 \sqrt{d})^{n+1}$ - נקבל

$$x_n + y_n \sqrt{d} < u + v \sqrt{d} < (x_1 + y_1 \sqrt{d})(x_n + y_n \sqrt{d})$$

$$1 < (u + v \sqrt{d})(x_n - y_n \sqrt{d}) < x_1 + y_1 \sqrt{d}$$

$$1 < (x_n u - y_n v \sqrt{d}) + \sqrt{d}(x_n v - y_n u) =: r + s \sqrt{d} < x_1 + y_1 \sqrt{d}$$

אשר זהו אלמנט של $r^2 - ds^2 = 1$ - נקבל $s < y_1$! $r < x_1$

אז קיבלנו סתירה להנחותינו של (x_1, y_1) .

⊙

קיבלנו שקבוצת הפתרונות היא חבורה ציקלית שנוצרת על ידי

הפיתרון הבסיסי (x_1, y_1) . אז נשאר לנו למצוא את הפיתרון
 הבסיסי והוא (p_{-1}, q_{-1}) הנשני ל x אויב המהפך של
 $\sqrt{d}$. זה אומנם לא בהכרח פשוט, אבל זה אפשרי ונסופי.

$$x^2 - 7y^2 = 1$$

פתרון

$$\sqrt{7} = [2, 1, 1, 1, 4]$$

$$\frac{p_{4k-1}}{q_{4k-1}} = ?$$

$$\frac{p_3}{q_3} = \frac{8}{3}$$

$$\frac{p_7}{q_7} = \frac{127}{48}$$

$$\frac{p_{11}}{q_{11}} = \frac{2024}{765}$$

לבוא (המא) אומרים N-9 38 11

6) גאומטריה של מרחבים

זה תחום שלחמצי "א" אינקהסי בסוף המאה ה-19. יש לו 6 מיני שימושים נחמדים. אנתנו נדבר על משוואה דיפרנציאלית.

נחפש פתרונות שלמים למשוואה $2x^2 + 10xy + 13y^2 = 1$
 בנקודה עם קואורדינטות שלמות פה $(0,0)$ שנקרא
 נאליקסה $2x^2 + 10xy + 13y^2 < 2$ היא פיתוח של המשוואה.
 האם אפשר זה שיהיה בזה אינסוף?

הצורה: קבוצה $C \subseteq \mathbb{R}^n$ תיקרא קמורה אם לכל $x, y \in C$
 $\{ (1-t)x + ty : 0 \leq t \leq 1 \} \subseteq C$ מתקיים
 קבוצה קמורה ב- $\mathbb{R}^n$ תיקרא קמור אם היא אינה
 מואב באל וזיזה (באחר כאל תחום מחימה נמוך $n-1$)
 קבוצה $C \subseteq \mathbb{R}^n$ נקראת סמטריה אם לכל $C \in C$ גם $-C \in C$.

הצורה: עבור קבוצה ב- $\mathbb{R}^n$ נגדיר את הנפח שלה (כדי
 נגדור העלון של סכום נפחי הקבוצות שאינן בזר אור
 בקבוצה. נסמן את הנפח של X ב- $Vol(X)$.

משפט זלא הולתה: לכל קמור חסום ב- $\mathbb{R}^n$ יש פה (ספי).

הצורה: שני בתוך $\mathbb{R}^n$ הם גם הקבוצה $\mathbb{Z}^n \subseteq \mathbb{R}^n$.

משפט 1 (משפט היאלי הקמור של אינקלסון):
 אם $C \subseteq \mathbb{R}^n$ קמורה וסימטרית נק $Vol(C) > 2^n$ אז קיימת
 ב- C נקודה שניג שאינה הראשית.

הוכחה: יהי $0 < t \in \mathbb{N}$. נבנום באוסל המישרים $\{ x_j = \frac{2a_j}{t} : j=1, \dots, n \}$
 נגדיר $a_j \in \mathbb{Z}$. המישרים מתחילים את $\mathbb{R}^n$
 חלקיהם n -מחצית בנפח $(\frac{2}{t})^n$ (כייה ציגה באונק $(\frac{2}{t})$).
 נסמן ב- $N(t)$ את מספר הקבוצות של קבוצה שנמצאים ב- C .

(28)

(נסמן ב- Z את המטריצה של מרחב וקטורי והבסיס. אז

$$\det(\Lambda) = \sqrt{\det(Z^t Z)}$$

אם השריג אלא אז Z רבועיג ואז $\det(\Lambda) = |\det Z|$

משפט 3: יהי $\Lambda \subseteq \mathbb{R}^n$ שריג אלא ויה $C \subseteq \mathbb{R}^n$ קטור.

סמטריג רק ל- $\text{Vol}(C) > 2^n \det(\Lambda)$ אז יש ב- C

נקודת שריג של Λ שאינה המשיג.

הוכחה: ויה $\{z_1, \dots, z_n\}$ בסיס של Λ . נגדיר $f: \mathbb{R}^n \rightarrow \mathbb{R}^n$

ע"י $f(x) = Zx$ ואשר Z המטריצה של מרחב וקטורי והבסיס.

$$f(x_1, \dots, x_n) = x_1 z_1 + \dots + x_n z_n$$

f תה"ע! $f(Z^n) = \Lambda$ (כמוכן f גם סגור מרחב וקטורי).

אם $K \subseteq \mathbb{R}^n$ בעל נפח $\text{Vol}(f(K)) = \text{Vol}(K) \cdot \det \Lambda$ (זו תוצאה

אמצעיתית ענאית).

$f^{-1}(C)$ קבוצה סמטריג קטורה, משיג שזו תכנה שזאברה

וגם סגור מרחב וקטורי ענאית.

$$\Rightarrow \text{Vol}(f^{-1}(C)) = \frac{\text{Vol}(C)}{\det \Lambda} > \frac{2^n \cdot \det \Lambda}{\det \Lambda} = 2^n$$

$\Leftarrow$ קיומ נקודת שריג של $f^{-1}(C)$ שאינה המשיג.

נסמן את הנקודה הזו ב- x . אז $f(x) \in C \cap \Lambda$ וזה בדיוק

אז שריגו. (29)

המשמור היא אומטריג של וידטרמיננטה של Λ היא הנפח

של האקסטרם (היסודי שנוצר ע"י הבסיס).

משפט 4: $\Lambda \subseteq \mathbb{R}^n$ שריג אמ"א Λ בוסקרטוג (כומר ט

נקודה היא אבוצה) ואצטמיר (כומר סאנה עתמור אלתוסור)

נקודה משה"י"יש לנו פה קשר בין קוטריון אסימטר לפרוטקטור.

הוכחה:

אם בסיס

$\Leftarrow$ יהי $\Lambda \subseteq \mathbb{R}^n$ שריג. בור משה"י"יש לנו אצטיבי.

נניח שהיא בוסקרטוג. נסמן ב- C את קוטריון הוויזיה (הפנתה ב- $\mathbb{R}^n$).

Z_C - הווייתו של C . $Z_C = \{Z_C : C \in C\} = f(C)$ (הפונקציה)

נלקחת לרוח לאינה 0 $z_m = m_1 z_1 + \dots + m_r z_r$ $z_1, \dots, z_r$

$$m_1, \dots, m_r = 0 \iff (m_1, \dots, m_r) \in C$$

$\Delta \cap (z + \mathbb{Z}C) \neq \emptyset$ רק סביבה פתוחה $z + \mathbb{Z}C$ $z \in \Delta$ שם

∴ $\text{AB} \parallel \text{CD}$ $\Rightarrow$

$\Rightarrow$ תהי $\Lambda \subseteq \mathbb{R}^n$ פסקרטיב וזגליות. (בתור) $z_i \in \Lambda$, $0 \neq z_j \in \Lambda$

אם הנחיצה של מודעותה הן $z_1, \dots, z_{j-1}$ ו- $|K_0|$ $L_j = \{ z_{j-1} y : y \in \mathbb{R}^{j-1} \} \subseteq \mathbb{R}^n$ תלוי בהנחות $z_1, \dots, z_{j-1}$

כל $\Lambda \setminus L_j = \emptyset$. אחת, נבחר $x \in \Lambda \setminus L_j$

יג) p האקסיומן הנזכר ע"י $x, y, \dots, z$, z ו z , z

$$P_j = \{ \lambda_1 z_1 + \dots + \lambda_{j-1} z_{j-1} + \lambda_j x : 0 \leq \lambda_i \leq 1 \}$$

Λ דיסקרטיוו - P_j קאנוניקאליסטישע. δ אפערטור (וויקלונג) - $\hbar$.

$\Delta \cap P_j$ הוא סופי וגם $\kappa \in \Delta \cap P_j$. $x \in \Delta \cap P_j$ (בתח

$\exists j \in P_j \cap \Delta$ ונקודת הקרבה ביניהם $\delta - j$ למינה j .

ק"מ - כן כי $P_j \cap \Delta$ סופי.

ז' אינו תלם עינאית בקאפא ו-ז', ... ז' כי בחינו אלו יק
שם עא (מנ) מניסור הנפול על ופ. כה נאליק. ז' ז'

שלא יישאו על א-יב לקחת. ברור זה שיתבאר ח"ב להערה.

(ראו, דוגמה של פונקציה $f: \mathbb{R} \rightarrow \mathbb{R}$ כזו שיש לה $\lim_{x \rightarrow \infty} f(x) = 0$ אבל f אינה מתכנסת ל-0 ב- ∞).

דוגמה) $\alpha_i \in \mathbb{Z}$ - כל מספרים שלמים. $X = \alpha_1 z_1 + \dots + \alpha_r z_r$

$$\Delta \ni x'' = x - x' = \dots \quad x' = \alpha_1 z_1 + \dots + \alpha_r z_r$$

$$= \{\alpha_1\} z_1 + \dots + \{\alpha_r\} z_r$$

$$Lr - N \quad x'' \in \mathcal{O} \text{ ונתון } x'' \in P_r \quad \Leftrightarrow \quad 0 \leq \{\alpha_i\} < 1$$

ה) $\text{Lr} - \text{N} - \text{Zr}$ על מנת להבדיל בין Lr ו- Zr

בלא תהיה סתירה למניחים נקבעה $\{d_r\} = 0$ בלתי

הצורה הכללית $\{\alpha_{r-1}\} = 0$ היא נכונה, $X'' = \{\alpha_1\}Z_1 + \dots + \{\alpha_{r-1}\}Z_{r-1} \in C$

(ii) $\wedge$ la oia $z_1, \dots, z_r$ nrb, i bd $\alpha_i \in \mathbb{Z}$

• $\Delta \Leftarrow$ Δ $\Leftarrow$

29

אשכנח 6: (פרמיר) אם $p \equiv 1 \pmod{4}$ אז קיימים

$$p = a^2 + b^2 \quad a, b \in \mathbb{N}$$

האותה: אם $p \equiv 1 \pmod{4}$ אז קיים $q \in \mathbb{N}$ כך

$$q^2 + 1 \equiv 0 \pmod{p} \quad (\text{זה אומר } -1 \text{ הוא ריבוע חסומה הרפואי})$$

אזכור p וזה נקרא אגף שני (3 קדמי)

$$\Lambda \subseteq \mathbb{R}^2 \text{ שמיס } \left\{ \begin{pmatrix} 1 \\ q \end{pmatrix}, \begin{pmatrix} 0 \\ p \end{pmatrix} \right\} \text{ א.}$$

$$C = \{ (x, y) \in \mathbb{R}^2 : x^2 + y^2 < 2p \} \quad \det \Lambda = p$$

פניה ברורים $\sqrt{2p}$ א

$$\text{Vol}(C) = \pi \cdot (2p) > 2^2 p = 2^2 \det \Lambda$$

(a) $\Leftarrow$ קיומה C (נקודה שיהיה Λ שאינה נראית, (b) נ"ח

$$\begin{pmatrix} a \\ b \end{pmatrix} = j \begin{pmatrix} 1 \\ q \end{pmatrix} + k \begin{pmatrix} 0 \\ p \end{pmatrix} \quad j, k \in \mathbb{Z}$$

$$a^2 + b^2 = j^2 + (qj + pk)^2 = j^2(1 + q^2) + k^2 p + 2jkqp \equiv 0 \pmod{p}$$

$$a^2 + b^2 = p \quad \Leftarrow \quad p \mid (a^2 + b^2) \quad ; \quad 0 < a^2 + b^2 < 2p$$

30

אשכנח 7: (פירמיר) אם $p \equiv 3 \pmod{4}$ אז קיימים

אגף שני (3 קדמי)

האותה: אם $p \equiv 3 \pmod{4}$ אז קיים $q \in \mathbb{N}$ כך

זה נקרא אגף שני (3 קדמי)

$$u^2 + v^2 + 1 \equiv 0 \pmod{p} \quad (\text{זה אומר } -1 \text{ הוא ריבוע חסומה הרפואי})$$

אזכור p וזה נקרא אגף שני (3 קדמי)

$$\Lambda \subseteq \mathbb{R}^4 \text{ שמיס } \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \det \Lambda = 1$$

$$C = \{ (x_1, x_2, x_3, x_4) \in \mathbb{R}^4 : x_1^2 + x_2^2 + x_3^2 + x_4^2 < 2p \}$$

$$\text{Vol}(C) > 2^4 p^2 = 2^4 \det \Lambda \quad \text{א}$$

$$p = x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv x_1^2 + x_2^2 (ax_1 + bx_2)^2 + (bx_1 - ax_2)^2 =$$

$$= (a^2 + b^2 + 1)(x_1^2 + x_2^2) \equiv 0 \pmod{p}$$

31

(סיני)

משפט זרימה: יהיו $Q \in \mathbb{Z}^+$ $\alpha \in (0,1)$ (זכור)

$$C = \{(x,y) \in \mathbb{R}^2 : x \in (Q-\frac{1}{2}, Q+\frac{1}{2}), |x\alpha - y| < \frac{1}{Q}\}$$

$$\text{Vol}(C) = (2Q+1) \frac{2}{Q} = 4 + \frac{2}{Q} > 4 = 2^2 \quad \text{זכור}$$

$$|x - \frac{p}{q}| < \frac{1}{qQ} : q < Q-1 \quad (q,p) \in \mathbb{Z}^2 \quad \Leftarrow \text{קיים}$$

היג גבנית מנייה ψ_i במשתנים $x_1, \dots, x_n$ עם מקצבים

$$\psi_i(x) = \sum_j \alpha_{ij} x_j = (\psi_i, x) \quad \alpha_{ij} \text{ משקל}$$

דמויות $\{\psi_i\}_{i=1}^n$ יותר מהתנאים נכסוס משקל Δ ואז ניתן להגדיר

אם C קבוצה קמורה חי

$$(תיבה) \quad C = \{x \in \mathbb{R}^n : \forall i |(\psi_i, x)| \leq \lambda_i, 0 < \lambda_i \in \mathbb{R}\}$$

$$\text{Vol}(C) = 2^n \prod_{i=1}^n \lambda_i / \det(\Delta) \quad \text{זכור}$$

$$\lambda_1 \dots \lambda_n \geq \det(\Delta) \Leftarrow \frac{2^n \lambda_1 \dots \lambda_n}{\det \Delta} \geq 2^n \det(\Delta)$$

$$0 \neq x \in \mathbb{Z}^n \cap C \quad \Leftarrow$$

נניח $Q(x) = \sum \alpha_{ij} x_i x_j$ גבנית ריבועית מוגדרת מילוי

אם צורת הריבוע $\Delta = \det(\alpha_{ij})_{ij}$ זכור (אם $\Delta > 0$)

$$\text{Vol}(C) = \int_{\mathbb{R}^n} \chi_C(x) dx = \int_{\mathbb{R}^n} \chi_{\{x: Q(x) \leq \lambda^2\}} dx$$

$$\int_{\mathbb{R}^n} \chi_{\{x: |y| \leq 1\}} dy_1 \dots dy_n = \frac{\pi^{n/2}}{\Gamma(\frac{n}{2}+1)} \quad \text{זכור}$$

$$\Gamma(\frac{n}{2}+1) = \begin{cases} (\frac{n}{2})! & \text{אם } n \text{ זוגי} \\ \frac{n}{2}(\frac{n}{2}-1) \dots (\frac{n}{2}-\frac{1}{2}) \sqrt{\pi} & \text{אם } n \text{ אי זוגי} \end{cases}$$

משפט אינקלסקי (אם Q קיים $0 \neq x \in \mathbb{Z}^n$ רק אם

$$Q(x) \leq 4 \int_{\mathbb{R}^n}^{-\frac{1}{2}} \Delta^{\frac{1}{2}}$$

אם השוויון הוא מתקיים

מפתחים שימוש מרכזי אף הנוקדה הכי קצרה בשריח.

נניח S שורש של פולינום ריבועי עם מקדמים שלמים, נניח S

$N = 10^5$ (אם x השורש של פולינום הווקטורים

25.12.04
תורה
המספרים

מספרים אגזוטיים

הגדרה: מספר α יקרא אגזוטי אם קיים פולינום לא טריוויאלי $P(x)$ עם מקדמים שלמים כך ש- $P(\alpha) = 0$.
מספר לא אגזוטי נקרא טרנסצנדנטי.

הערה: יש מא פולינומים במקדמים שלמים, לכן יש מא מספרים אגזוטיים. לכן יש א מספרים טרנסצנדנטיים. (האבסורד היא שההבדל יתכן קשה להבחין על מספר טרנסצנדנטי).

$$\begin{aligned} \alpha = \sqrt{2-\sqrt{3}} &\Leftrightarrow \alpha^2 = 2-\sqrt{3} \Leftrightarrow 2-\alpha^2 = \sqrt{3} \\ &\Leftrightarrow (2-\alpha^2)^2 = 3 \Leftrightarrow \alpha^4 - 4\alpha^2 + 1 = 0 \\ &\Leftrightarrow \alpha \text{ שורש של } P(x) = x^4 - 4x^2 + 1 \text{ עם קוטר אגזוטי.} \end{aligned}$$

הערה: לא כל המספרים האגזוטיים ניתנים לתיאור (ניתנה ע"י נוסחה סגורה) הם שלמים ופעולות על רציונליים. למשל $x^5 - 6x + 2$ לא ניתן לתיאור.
אין פתחנות ראוי.

הגדרה: הגובה של פולינום P אגזוטי α הוא $H(P) = \max_{0 \leq i \leq n} |a_i|$ כאשר a_i המקדמים של P .

סיווג: (סמן ב- $P_\alpha(x)$ את הפולינום האינמינלי של α - $P_\alpha(\alpha) = 0$).
(גודל α הנדרג של α זהו $d = \deg \alpha = \deg P_\alpha(x)$)

נחזיר $0 < D, H$ מספרים ממשיים כך ש- $H(P) \leq H$ ו- $d \leq D$.
קל לראות שקיים מספר סופי של פולינומים שמקדמיהם אינן הגדולות מ- H .
לכן קיים מספר k אחיד של פולינומים עם מקדמים שלמים. כל פולינום אמיתי H יש לו חזית H שונים ולכן חזית המספרים האגזוטיים היא M .
היא M לכן חזית קבוצת המספרים הטרנסצנדנטיים היא A .

הערה: $\frac{p}{q}$ חסר רציונל. הוא אלמנטי מצומד $\perp$ כי היות
אם הפולינום $q \cdot x - p = 0$.

משפט צורנו: אם α אלמנטי מצומד $1 < d$ קיים $0 < c < 1$ הכולל
קב-ה- α רק שמתקיים אם $\frac{p}{q} \in \mathbb{Q}$ $|\alpha - \frac{p}{q}| > \frac{c}{q^d}$.

הוכחה: יהי $P_\alpha(x)$ הפולינום המינימלי של α . α צמוד חזק הממוצע
 $-P_\alpha(\frac{p}{q}) = P_\alpha(\alpha) - P_\alpha(\frac{p}{q}) = (\alpha - \frac{p}{q}) P'_\alpha(\xi)$

חזור ξ בין $\alpha - \frac{p}{q}$ ו- α .

אם $|\alpha - \frac{p}{q}| \geq 1$ אז מתקיים $0 < c < 1$ בד $|\alpha - \frac{p}{q}| > \frac{c}{q^d}$
אם $|\alpha - \frac{p}{q}| < 1$:

ξ בקטע $[\alpha-1, \alpha+1]$ $P'_\alpha(x)$ חסומה (כי היא רציפה על קבוצה

קומפקטית) ולכן קיים $1 < m$ כך ש- $P'_\alpha(\xi) < m$

ב $P_\alpha(\frac{p}{q}) \neq 0$ כי אחרת זו סתירה למינימליות של P_α (כי נוס אחר

גדול ה- $\alpha - \frac{p}{q}$ מתקבל אנה $q(x)$ שגובה קטנה מ- d והיא
מאפשרת α).

$$|P_\alpha(\frac{p}{q})| = \left| \frac{a_0 q^d + a_1 q^{d-1} p + \dots + a_d p^d}{q^d} \right| \geq \frac{1}{q^d} \quad \text{ע}$$

כי המונה הוא מספר שלם שאינו אפס.

$$q^d m |\alpha - \frac{p}{q}| \geq |q^d P_\alpha(\frac{p}{q})| \geq 1 \quad \text{ב ראי ע'}$$

אפיון של $\frac{1}{q^d}$
הממוצע בשווה עם m
שגובה חסומה ξ מ

ב נבחר $0 < c = \frac{1}{m} < 1$ וסיימנו. $\odot$

למשל ניקח c איזוהי צומד c - d . מתקיים $|\alpha| < 1 + |\alpha|$

$$c = \frac{1}{d^2(1+|\alpha|)^{d-1}H(\alpha)} \quad \text{דבר} \quad P'_\alpha(x) < \frac{1}{c}$$

ע"י רציונליים

אפס זווהו אחר שאי אפשר לקרוב יותר אפיון טוב אפסנים אלמנטריים. $\checkmark$ אב

אם יש מספר שגובה לקרוב אולי טוב ע"י רציונליים הוא תיכ אחר
אנטיסוציאלי. תכל נפרטת אב לזה.

32

הצגה: מספר ממשי α יקרא מספר ליונדל אם $\alpha \in \mathbb{R}$ ומתקיים

שלב $n \in \mathbb{N}$ קיימים $p_n, q_n > 1$ כך של- $|\alpha - \frac{p_n}{q_n}| < \frac{1}{q_n^n}$

משפט: מספר ליונדל הם סתם צפופים $\mathbb{R}$.

הוכחה: יהי α מספר ליונדל. נניח שיש איבר d אפריורי.

אם משפט ליונדל קיים $0 < c < 1$ כך של- $|\alpha - \frac{p}{q}| > \frac{c}{q^d}$

לכל $\frac{p}{q}$. גודל α מספר ליונדל. נבחר $k \geq d + \frac{\log(1/c)}{\log 2}$

אז מתקיים $\frac{c}{q^k} < |\alpha - \frac{p_k}{q_k}| < \frac{1}{q_k^k}$ אבל זה לא יתכן אחרת

לפי הבחירה של k . (11)

דוגמה: $\alpha = \sum_{n=1}^{\infty} 10^{-n!}$. זה מספר שפרטית העשרוני שלו מאידך

דליל - רק במקומות ה- $n!$ אחרי הנקודה אנחנו 1 וכל השאר 0.

זה מספר עם רציונל + כי הפרטית שלו לא מתכנסת.

בהינתן $n \in \mathbb{N}$ נבחר $p_n = 10^{n!} \sum_{k=1}^n 10^{-k!}$

וכי $q_n = 10^{n!}$

$|\alpha - \frac{p_n}{q_n}| = \sum_{k=n+1}^{\infty} 10^{-k!} < \frac{2}{10^{(n+1)!}} < \frac{1}{(10^{n!})^n} = \frac{1}{q_n^n}$

α מספר ליונדל אך אינו אלגברי.

$T = \{ \sum_{k=1}^{\infty} a_k 10^{-k!} : a_k \in \{1, 2\} \}$ (גזיר)

פונקציה צומת מאינסוף תראה ש- T קבוצה מספר ליונדל. כמו כן, נניח

ש- $|T| = \aleph$ אז קבוצת מספר ליונדל היא עצמה הרצף.

משפט: (אורנס 1962)

כל מספר ממשי x ניתן להצגה כסכום א כחציה של שני מספרים

ליונדל α, β $x = \alpha + \beta = \alpha' + \beta'$ כאשר $\alpha, \beta, \alpha', \beta'$ מספרים ליונדל.

הוכחה: נניח רק על-הם הסכום למקרה ש- x איננו צינעל. בין 0 ל-1.

קיים $x = \sum_{j=1}^{\infty} x_j 2^{-j}$ פיתוח במסלול בעינינו. כאשר $x_j \in \{0, 1\}$

$\beta_j = x_j - \alpha_j$ $\alpha_j = \begin{cases} x_j & \text{אם } x_j \neq 0 \\ 0 & \text{אם } x_j = 0 \end{cases}$ (גזיר)

$\beta = \sum_{j=1}^{\infty} \beta_j 2^{-j}$ $\alpha = \sum_{j=1}^{\infty} \alpha_j 2^{-j}$

מאפשרים
הצגה כסכום
ליונדל

sk מתקיים $\gamma = \alpha + \beta$. נרצה להראות ש- α, β מספרים איраליים .

נניח ש- (α_j) אינסופית ונקבל עבור $1 \leq m$

$$0 < \alpha - \sum_{j=1}^{(2m)!-1} \alpha_j 2^{-j} = \sum_{j=(2m)!}^{\infty} \alpha_j 2^{-j} < \frac{1}{2^{(2m)!-1}}$$

יש אינסוף מספרים ...

משפט (Hermite) e מספר טרנסצנדנטי

φ ראשי, נסכים ש- e היא אינציונלית. אם $q = \sum_{n=0}^{\infty} \frac{1}{n!}$ (זהו)

ב- $q!$ ונקבל $(q-1)! p = q! \left(\sum_{n=0}^q \frac{1}{n!} + \sum_{n=q+1}^{\infty} \frac{1}{n!} \right)$

אם $q! \sum_{n=q+1}^{\infty} \frac{1}{n!} \in \mathbb{Z}$ ו- $(q-1)! p \in \mathbb{Z}$

$$q! \sum_{n=q+1}^{\infty} \frac{1}{n!} = \frac{1}{q+1} + \frac{1}{(q+1)(q+2)} + \dots < 1$$

2

ולו סתירה

הרעיון

גדיר $\Phi(t) = \int_0^t e^{tx} f(x) dx \quad t \geq 0$

ראשון $f(x)$ פולינום ממעלה m . f אינטגרלית בהתקיים (נקבל)

$$\Phi(t) = -e^{t-x} f(x) \Big|_{x=0}^t + \int_0^t e^{t-x} f'(x) dx$$

באינדוקציה על m (נקבל)

$$\Phi(t) = e^t \sum_{j=0}^m f^{(j)}(0) - \sum_{j=0}^m f^{(j)}(t)$$

נסמן ב- F את הפולינום המתקבל מ- f ו- f' והוא מספר המעצמים

העצמים המוחלטים של f .

$$|\Phi(t)| \leq \int_0^t e^{t-x} |f(x)| dx \leq t e^t F(t)$$

נניח ש- e אינציונלית ממעלה d . sk קיימים

$$\sum_{k=0}^d a_k e^k = 0$$

יב שמחב"פ

$$f(x) = x^{p-1} \prod_{\ell=1}^d (x-\ell)^p$$

בהינתן p גדיר

הדרגה של $f(x)$ היא $(d+1)p - 1 = p-1 + dp$

$$J = \sum_{k=0}^d a_k \Phi(k)$$

נניח כי $1 \leq k \leq d$ גדיר k

$$g_k(x) = \frac{f(x)}{(x-k)^p} = x^{p-1} \prod_{\substack{\ell=1 \\ \ell \neq k}}^d (x-\ell)^p$$

32

פונקציות $g_k(x)$ ו- p מספר ראשוני

$$f^{(j)}(x) = \sum_{i=0}^j \binom{j}{i} ((x-k)^p)^{(i)} (g_k(x))^{(j-i)}$$

אם $j \geq p$ אז $f^{(j)}(k) = 0$ מכיוון ש- $j < p$

$$f^{(j)}(k) = \binom{j}{p} p! g_k^{(j-p)}(k)$$

אם $j < p$ אז $f^{(j)}(k) = \binom{j}{j} g_k^{(j)}(k)$

באופן דומה $f^{(j)}(0) = \binom{j}{p} h^{(j-p)}(0) p!$ אם $j \geq p$ ו- $f^{(j)}(0) = 0$ אם $j < p$

$$\left(\prod_{e=1}^d (x-e)^p = \right) h(x) = \frac{f(x)}{x^{p-1}}$$

$h(x)$ פונקציה ממעלה d ו- $h(0) = (-1)^d (d!)^p$

אם $j > 0$ אז $h^{(j)}(0) = (-1)^{d-p} (d!)^p$

אם $j = p-1$ אז $f^{(j)}(0) = p! h^{(j-p)}(0)$

אם $j < p-1$ אז $f^{(j)}(0) = 0$

אם $p > d$ אז

$$J = - \sum_{k=0}^d a_k \left(e^k \sum_{j=0}^m f^{(j)}(0) - \sum_{j=0}^m f^{(j)}(k) \right) =$$

$$= - \sum_{j=0}^m \sum_{k=0}^d a_k f^{(j)}(k)$$

$J \neq 0$ מכיוון ש- $J \geq (p-1)!$ ו- $(p-1)!$ אינו מתפצל ב- p

$J \bmod p = a_0 f^{(p-1)}(0) \neq 0$

$$F(k) < k^{p-1} \prod_{e=1}^d (k+e)^p < (2d)^m$$

$$|J| \leq \sum_{k=0}^d |a_k| k e^k F(k) \leq H\left(\frac{e^d}{2}\right) d(d+1) (2d)^m \leq$$

$$\leq C^p$$

אם e מספיק גדול אז

$$(p-1)! \leq |J| \leq C^p$$

אם p מספיק גדול אז

33

לפי הטיעון

שיעור השלמה סיני.

פאנארמ

נניח $E = \{b_i\}$ מסת מניתיים וקטורי סת Λ ראני E .

$$\det(\Lambda) \leq \prod_{i=1}^n |b_i| \leq \frac{2^n}{J_n} \det(\Lambda)$$

$$J_n = \frac{\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2}+1)}$$

ראשי n גזל קלס מאלו למצא מסת כח, רהפסט וקח המון למן.
 אנתוני וראק אלתית למצא מסת למקיים מסת קרוב למס E .

הצעה: יני $\{z_i\}$ מסיס $|N|$ z_j^x אה הווקטור למתקנה

$$\mu_{ij} = \frac{(z_i, z_j^x)}{(z_j^x, z_j^x)}$$

 $\{z_i\}$ וקרא מסיס ממוצם L^3 אה מתקיימים (התנאים המסויים):

$$|\mu_{ij}| \leq \frac{1}{2} \quad (i)$$

$$|z_i^x + \mu_{i,i-1} z_{i-1}^x|^2 \geq \frac{3}{4} |z_{i-1}^x|^2 \quad (ii)$$

$$|z_i^x|^2 \geq (\frac{3}{4} - |\mu_{i,i-1}|) |z_{i-1}^x|^2 \quad (iii)$$

$$\det(\Lambda) \leq \prod |z_i| \leq 2^{\frac{n(n-1)}{4}} \det(\Lambda)$$

מסוס כח מקיים

$$|z_i| \leq 2^{\frac{n(n-1)}{4}} \det(\Lambda)^{\frac{1}{n}}$$

הע"ר המספר השלם הקטן - עבור $\alpha_1, \dots, \alpha_m \in \mathbb{Q}$ $\varepsilon, Q \in \mathbb{R}$
 ונניח למצא $\{q_i\} \in \mathbb{Z}$ כן של $q_i < Q$

$$|\sum q_i \alpha_i| \leq \varepsilon$$

(משפט מנקלמס) אם קטור $\alpha_i \in \mathbb{R}$ מסת $Q \geq \varepsilon^{-\frac{1}{m}}$
 עבור קבוע ε שלם. וניח $Q \geq \varepsilon^{-\frac{1}{m-1}}$ $\alpha_i = 1$ $0 < \varepsilon < 1$
 מסת $\mathbb{Q}$ המסוייה

$$M = \begin{pmatrix} 1 & \alpha_2 & \dots & \alpha_m \\ 0 & \varepsilon & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & \varepsilon & 0 \end{pmatrix}$$

יני Λ השלם הנפיש E וקטורי העמודות.

$q \in \mathbb{Z}^m$ וקטור בעל ערכים שלמים $qM = z \in \Lambda$ כאשר $M = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$
 אם $0 \neq |z| \leq \varepsilon$ אז $qM = z$ עבור q מסוים אחד
 פיתרון: נחלק $q_i < Q$ עבור $i \geq 2$

משפט: L^3 סדרה של סדרות Λ אז $\det \Lambda \leq \prod |z_i| \leq 2^{\frac{n(n-1)}{2}} \det \Lambda$ מתקיים
 הוכחה: דפוף ההצגה

$$|z_i|^2 = |z_i^*|^2 + \sum_{j=1}^{i-1} \mu_{ij}^2 |z_j^*|^2 \leq$$

$$\leq |z_i^*|^2 + \frac{1}{4} \left(\sum_{j=1}^{i-1} |z_{i-j}|^2 \right)$$

$$|z_j^*|^2 \geq \frac{1}{2} |z_{j-1}^*|^2$$

$$\Rightarrow |z_j^*|^2 \leq 2^{i-j} |z_i^*|^2$$

$$|z_i|^2 \leq 1 + \frac{1}{4} (2 + \dots + 2^{i-1}) |z_i^*|^2 \leq 2^{i-1} |z_i^*|^2$$

$$\Rightarrow \det(\Lambda) = \prod |z_i^*| \leq \prod |z_i| \leq 2^{\frac{n(n-1)}{2}} \prod |z_i^*| = 2^{\frac{n(n-1)}{2}} \det(\Lambda)$$

☺

הערות:

אם Λ הוא סדרה

www.nada.kth.se/~johanh/algnotes.pdf

67 3/11

תלדה נאספריס אאריי

היום נלחם ע. פ. צוקרמן.

קראם נצחיי א'ק ה'נחנ' ~~ש~~ א'ר ה'נחנ' צ'נ'ס'י'ר ש' e

פראשני, אספן זינן וואס הסתכלען אנה ביטד J

$J = \int \dots \leq C^p$ e) μ_K and ν_K are $\mathbb{R}^N$

15) האם קיים p ראשוני $J = \sum \dots \geq (p-1)!$, על ידי

סתיירה.

הערה: $x \in \mathbb{C}$ "קרא לזה" x הוא שורש של פולינום

הפונקציה $f: \mathbb{R} \rightarrow \mathbb{R}$ נתונה על ידי $f(x) = x^2 + 2x + 1$. מצא את $f(3)$.

משפט: המרחקים האמצעיים מהווים לצה,

הקדמה: אם x איננה אף הפולינום המניח'ל x היה הפולינום

והמתקן מצידה הקטנה ביותר מסל $\mathbb{Q}$ של מסל אחר X .

צורת הפתרון ה"מניח" $x \in \mathbb{C}$ אף $x \in \mathbb{R}$ א"פ

הערה: מעורבים גם "קטל" של אדם אחד או יותר והחלוקה

הנה פתרון ל- x עם פונקציות נגזרות. $\square$ וזהו תשובה

מסע: השלמים ואלמנטריים הם חלק

• a և b ամբողջ թվեր $a, b \in \mathbb{Z}$ թվեր: Օճեն

הצורה: יהיו משתנים $\alpha_1, \dots, \alpha_n$. הפולינום n -משתנים

$$C_k \in \mathbb{Q} \quad \sum_{k=1}^n C_k \alpha_1^{a_{1k}} \dots \alpha_n^{a_{nk}} = P(\alpha_1, \dots, \alpha_n)$$

$$\sigma \in S_n \quad \int_{S_0 = 1}^n P(\alpha_1, \dots, \alpha_n) = P(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)}) \quad \text{pk} \rightarrow \text{UNO (C)}^*$$

$$S_0 = 1$$

$$S_1 = \sum_{i=1}^n \alpha_i$$

העמודים הראשונים הם חלק מהספר הראשון והשני.

$$S_2 = \sum_{i < j} \alpha_i \alpha_j$$

$$S_n = \alpha_1 \dots \alpha_n$$

$$(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n) = \sum_{j=0}^n x^j S_{n-j} (-1)^{n-j} \quad \text{נשים ר"ל שמתקיים}$$

משפט: אם $P(\alpha_1, \dots, \alpha_n)$ פולינום סימטרי ב- α_i לכן Q ש"ל

$P_1(S_1, \dots, S_n)$ Q לכן S_i ה-פולינום

$$P(\alpha_1, \alpha_2) = \alpha_1^2 + \alpha_2^2 = (\alpha_1 + \alpha_2)^2 - 2\alpha_1\alpha_2 = S_1^2 - 2S_2 \quad \text{בדוגמה}$$

משפט: אם P פולינום לכן Q ש"ל $\alpha_1, \dots, \alpha_n$

! $Q(\alpha_1, \dots, \alpha_n)$ פולינום סימטרי Q ש"ל $Q(x_1, \dots, x_n)$!
אם רצונם.

הוכחה: מהמשפט הקודם מספיק להראות עבור $Q = S_i$

ואם S_i פולינום i מתקדם פולינום לכן Q ה- S_i

$$P(x_1, \dots, x_n) = h(x-\alpha_1)\dots(x-\alpha_n) = h \sum_{j=0}^n x^j S_{n-j} (-1)^{n-j} \quad \text{אם}$$

ש"ל S_i הם בסיס ומהקודם של P הם רצונם.

②

משפט: π סימטרי

$$I(t) = \int_0^t e^{t-x} f(x) dx = \quad \text{הנחה}$$

$$= e^t \int_0^t e^{-x} f(x) dx = e^t \int_0^1 e^{-\lambda t} f(\lambda t) t d\lambda =$$

$$= t \int_0^1 e^{(1-\lambda)t} f(\lambda t) d\lambda$$

$$F(x) = \sum_{j=0}^m f^{(j)}(x) \quad \text{אם } f \text{ פולינום ממעלה } m \text{ ורצוי}$$

$$\Rightarrow \frac{d e^{-x} F(x)}{dx} = -e^{-x} F(x) + e^{-x} \sum_{j=0}^m f^{(j+1)}(x) = -e^{-x} f(x)$$

$$= \sum_{j=1}^{m+1} f^{(j)}(x) = \sum_{j=1}^m f^{(j)}(x)$$

$f^{(m+1)}(x) = 0$

$$\Rightarrow \int_0^x -e^{-y} f(y) dy = e^{-x} F(x) - F(0)$$

$$\Rightarrow -I(x) = -\int_0^x e^{x-y} f(y) dy = F(x) - e^x F(0)$$

36

$$|I(x)| = \left| x \int_0^1 e^{(1-x)x} f(\lambda x) d\lambda \right| \leq$$

$$\leq |x| \int_0^1 |e^x| |f(\lambda x)| d\lambda \leq |x| M e^x$$

$\downarrow$
 $M = \max_{0 \leq \lambda \leq 1} |f(\lambda x)|$

נניח שיש לנו π -פולינום P כזה ש- $P(i) = 0$ לכל $i \in \mathbb{Z}$.
 (כלומר P מתאפס בכל האינטגרים).

יהי P הפולינום המינימלי של $i\pi$ ויהיו $\alpha_1, \dots, \alpha_d$ השורשים של P ונניח $\alpha_1 = i\pi$. נסתכל על המרחב הנמוס P .

$$\Leftrightarrow e^{i\pi} + 1 = 0$$

$$0 = (e^{\alpha_1} + 1)(e^{\alpha_2} + 1) \dots (e^{\alpha_d} + 1) = \sum e^w$$

$$w = \delta_1 \alpha_1 + \dots + \delta_d \alpha_d \quad \delta_i \in \{0, 1\}$$

כלומר w הוא סכום של α_i (כמה פעמים). נניח $\beta_1, \dots, \beta_n$ הם השורשים של P .

$$0 = \sum_{j=1}^n e^{\beta_j} + (2^d - n) \cdot 1$$

$$2^d - n = k > 0$$

$$f(x) = x^{p-1} \prod_{j=1}^n (x - \beta_j)^p$$

$$\deg f = p-1 + np$$

$$\Rightarrow F(x) = \sum_{j=0}^{p-1+np} f^{(j)}(x)$$

$$L = \sum_{j=1}^n (F(\beta_j) - e^{\beta_j} F(0))$$

$$|F(\beta_j) - e^{\beta_j} F(0)| \leq |\beta_j| \max_{0 \leq \lambda \leq 1} |f(\lambda \beta_j)| e^{\beta_j}$$

$$|f(\lambda \beta_j)| \leq (|\lambda \beta_j| + 1)^p \prod_{m=1}^n (|\lambda \beta_j - \beta_m|)^p = O(\beta_j)^p \leq C^p$$

$$\sum_{j=1}^n F(\beta_j) = p! A$$

$$\sum_{j=1}^n F(\beta_j) = p! A$$

$$(hg)^{(m)} = \sum_{k=0}^m \binom{m}{k} h^{(k)} g^{(m-k)}$$

$$f^{(m)}(x) = \sum \binom{m}{k} [(x - \beta_j)^p]^{(k)}$$

$$\Rightarrow f^{(m)}(x) \Big|_{x=\beta_j} = \underbrace{\binom{m}{p}}_{\substack{\text{אולי לא} \\ \text{נכון} \\ \text{לכאן}}} p! \left[x^{p-1} \prod_{\substack{j=1 \\ j \neq j}}^n (x - \beta_j)^p \right]^{(m-p)} \Big|_{x=\beta_j}$$

נניח ש- α_j שלם (אם צריך)

$$l_{\beta_j} = l(\alpha_{j_1} + \dots + \alpha_{j_g})$$

$$0 = P(\alpha_j) = \sum_{q=0}^d c_q \alpha_j^q = \sum_{q=0}^d c_q l^{d-1} \alpha_j^q =$$

$$= \sum_{q=0}^{d-1} c_q (l \alpha_j)^q \underbrace{l^{d-1-q}}_{\text{שלם}} + (l \alpha_j)^d$$

נציין, אם כן פולינום המקדמים שלמים של α_j מתפצל.
 $\Leftarrow$ נניח שלם אחר. נחלק שלמים אלו זהים הם חוק
 נובע ש- A שלם אחר. (נניח זמנא) ש- A רציונלי.
 מספיק להראות ש- $A \in \mathbb{Q}$ רציונלי.

$$f(x) = x^{p-1} \prod_{j=1}^n (lx - l_{\beta_j})^p$$

המקדמים של f הם פולינומים סימטריים ב- β_j וכן $\mathbb{Q}$.
 אם ניקח אתם באמצעות הפולינומים הסימטריים הנוספים
 ב- β_j .

$$\prod (x - w) = x^k \cdot \prod_{j=1}^n (x - \beta_j)$$

$\prod (x - w)$ סימטרי ב- w אם מקדמיו (יתרים) רציונליים
 הפולינומים הפולינומים הסימטריים הנוספים ב- β_j שהם המקדמים
 של P (הזו רציפה ב- l). $\Leftarrow$ המקדמים של f
 רציונליים $\Leftarrow$ המקדמים של f (הזו רציפה ב- l) $\Leftarrow$ המקדמים
 של סכום הנגזרות רציונליים $\Leftarrow$ המקדמים של $F(x)$ רציונליים.
 $\Leftarrow$ $\sum F(\beta_j)$ פולינום סימטרי ב- β_j וכן $\mathbb{Q}$ אם רציונלי.
 $\Leftarrow$ $\sum F(\beta_j) = p \cdot A$ עבור A שלם.

נחזור ל- $\sum F(\beta_j) + \sum e^{\beta_j} F(0)$ (נניח להפיל) ש- $\sum e^{\beta_j} F(0)$ מתחלק
 ב- $(p-1)!$ אם $k \neq 0$ וכן $\sum_{j=1}^n e^{\beta_j} = k \neq 0$ אם $\sum_{j=1}^n e^{\beta_j} F(0)$ מתחלק ב- $(p-1)!$ אם $k \neq 0$.
 (ראו ש- $f^{(m)}(0)$ מתחלק ב- $(p-1)!$ בדיוק זה)
 $f^{(m)}(0) = \binom{m}{p-1} (p-1)! \left[\prod_{j=1}^n (lx - l_{\beta_j})^p \right]^{(m-p+1)} \Big|_{x=0}$
 מאותם שקולים כמו קודם וראו ש- $f^{(m)}(0) \mid (p-1)!$ (שזה אחרת) ש-
 $F(0) = \sum_{j=0}^{p-1} f^{(j)}(0)$ לא מתחלק ב- p . אם לזה לא ממש (שזה לא...

8.1.04
תורת
המספרים

לימוד עם נחם

על סדרה יים:

חללה קצרה

והצורה משפטים רג'

משואל Thue

בתחנות רציונליים משואל

תקלימים אלפיטיים

ף

אז חרשיו רכני את המספטים החסויים:

צורה $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ איש מספר אינסופי של $\frac{p}{q}$ רק ל- $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$

$\alpha \in \mathbb{Q}$ אם $\epsilon < \delta$ יש רק מספר סופי של $\frac{p}{q}$

המקיימים $|\alpha - \frac{p}{q}| < \frac{1}{q^{2+\epsilon}}$

למה אם $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ אזי מספר מחרה $d > 1$ קיים $c \in (0, 1)$ רק

אם $\frac{p}{q}$ רציונלי מוקים $|\alpha - \frac{p}{q}| > \frac{c}{q^d}$

החיסוק הסבו היה של Roth משנת 1955 ושה זוכה אולי
נפס Fields.

משפט רג': אם $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ אזי מספר מחרה $d > 1$ אם $0 < \epsilon$

קיים רק מספר סופי של $\frac{p}{q} \in \mathbb{Q}$ רק ל- $|\alpha - \frac{p}{q}| < \frac{1}{q^{2+\epsilon}}$

קיימה: $\sum 10^{-3^n}$ זה מספר שגבש סקרה מחרה 3

לפס מספר חזר א-2 ולכן ארכוסצונג-2.

מקרה פרט של משואל Thue

$x > y$ מהם $x^3 + y^3 = n$ $n \in \mathbb{N}$, $x, y \in \mathbb{N}$

נשתמש בנוסחה רג' מקורר:

$$x^3 + y^3 = (x+y)(x^2 - xy + y^2)$$

מאתר ל- $x, y \in \mathbb{N}$ הפירוק הוא מילימים.

$$B = x^2 - xy + y^2 \in \mathbb{Z} \quad A = x+y \in \mathbb{Z} \quad (NO)$$

$$B = x^2 - xy + y^2 = x^2 - x(A-x) + (A-x)^2$$

$$\Rightarrow 3x^2 - 3Ax + A^2 - B = 0$$

למים A, B

$$\Rightarrow x_{1,2} = \frac{3A \pm \sqrt{9A^2 - 12(A^2 - B)}}{6} =$$

$$= \frac{3A \pm \sqrt{12B - 3A^2}}{6}$$

אם יוצא ל- x שלם אז קיבלנו פיתרון ממילארי.

$$7 \cdot 13 \cdot 19 = n = 1729$$

הפירוקים הראשונים הם $A=7, B=13$ $A=13, B=19$

אחרים

$$A=4, B=13 \cdot 19$$

$$A=13, B=7 \cdot 19$$

מתברר שעבור $A=13$; $B=133$ (קטן)

$$y=4, x=12$$

וכן עבור $A=19$ $B=91$ (קטן)

$$x=10, y=9$$

$$12^3 + 1^3 = 1729 = 10^3 + 9^3$$

למעשה זה המספר הראשון שניתן לפירוק לסכום חזקות של שני בסיסים אופנים שונים.

מקרה כללי של משוואה Thue

$$ax^3 + by^3 = m \quad a, b, m \in \mathbb{Z} \text{ איזו משוואה}$$

ישנו רק מספר סופי של פתרונות שלמים

הזרה: מותר ל- x^3, y^3 יגלים להיות שליליים אך עולה

פה סוגיית הסופיות. הרי למשל - $ax^2 + by^2 = m$ בולטאי'ל

רק מספר סופי של פתרונות שלמים $ax^2 + by^2$ חזוי (זהו משפט

מסויי'ם פשוט $ax^2 + by^2 > m$ ואין מה לחפש חוץ

הולחה:

(*) נניח $a=1$, שלם b פיתרון (x, y)
 $x^3 + a^2by^3 = a^2m$ למשוואה (ax, y) ישנה פיתרון

עקומים אליפטיים

יהי $P(x, y)$ פולינום מעוקם ע"א סימולר + מתהר כי (י) $P(x, y)$ ע"י ההצגה שלמים כ -

$$y^2 = x^3 - Ax + B$$

עקומים מצוה זו נקרא עקום אליפטי.

סעיף: יהא E עקום אליפטי הנותק ישר וצ"ל L במישור $\mathbb{R}^2$

(ישר מהצורה $ax+by+c=0$ ושל $a, b, c \in \mathbb{Q}$)

אזי במקרה הכללי תיתקבלנה 3 נקודות חיתוך רק שאם שתיים מהן וצ"ל יי-אז השלישית וצ"ל יי-אז

הנחתו הנותק של E : L - היא

$$\{(x, y) : y^2 = x^3 - ax + b, cx + dy = e\}$$

אם (ח) φ אחר χ נקרא פונקציה $r(x)$ ממעלה שלישית $\mathbb{Q}$.

לכך החיתוך הוא במקרה של 3 נקודות שונות $\{(x, y)\}^3$

נציג $r(x)$ כ - $r(x) = \prod (x - x_i)$ $(x - x_1)(x - x_2)(x - x_3)$

$\Leftarrow$ אם $x_1, x_2 \in \mathbb{Q}$ אז $x_3 \in \mathbb{Q}$. (י)

אנחנו נקרא נחשן על הרכבה: הנוצק $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$

אם יש וצ"ל L נותן פהגדיר את ההרכבה $P_1 \circ P_2$

במיד הנקוצה השלישית $P_3 \notin L$.

יש פה כמה בעיות: L ע"א תמיד תותק ב-3 נקודות: וזה אלו

שהוא משיק ל- E ב- P_1 וזה אלו שהוא אנכי.

אם L משיק ל- E בנקודה P_4 אז נגדיר את נקודת החיתוך

השנייה אלו $P_1 \circ P_2$.

בשמים ע"פ מושגים האנכיים נוסף נקודה אינסוף ∞ והיא

הזה בל הישרים האנכיים. זאת גם הנקודה השלישית איבר

היחידה בחבורה.

בהינתן P_1, P_2, P_3 נותק $P_1 + P_2 + P_3 = \infty$ אמרנו הן עוקבות

אם אלו יש. על החבורה היא $P_1 + P_2 = (x_3, -y_3)$

משפט Mordell מראה כי מקורה של המשוואה
אנטיגון נוצרה סופית.

השערת abc

דינה זליגר

הבעיה העשירית של הילברט

הבעיות של הילברט (Hilbert) הן רשימה של 23 בעיות פתוחות במתמטיקה, שהוצגה על-ידי המתמטיקאי דיוויד הילברט ב-8 באוגוסט 1900 בוועידת פריז של הקונגרס הבינלאומי של המתמטיקאים. כל השאלות שהוצגו לא היו פתורות באותה תקופה. שאלה אחת מעניינת במיוחד:

למצוא אלגוריתם שיקבע האם למשוואה פולינומיאלית במקדמים שלמים קיים פיתרון טבעי או לא.

השאלה לא לגמרי ברורה משום שאין הגדרה ברורה של המושג אלגוריתם. אם נאמץ את השימוש במכונת טיורינג נקבל שאלגוריתם הוא תהליך סופי שיכול להיות ממומש בעזרת תוכנית מחשב שמורכבת ממספר סופי של פעולות מתמטיות ובסופה ניתנת תשובה חיובית או שלילית.

בשנת 1970 הוכח שלבעיית העשירית של הילברט אין פיתרון, כלומר לא קיים אלגוריתם שבהינתן פולינום קובע בזמן סופי אם יש לו פתרון טבעי או לא.

הגדרה: קבוצה $A \subset \mathbb{N}^m$ של m -יות של מספרים שלמים חיוביים נקראת **דיופנטית** אם קיים פולינום $P \in \mathbb{Z}[X_1, \dots, X_n, Y_1, \dots, Y_m]$ כך שלמשוואה $P(X_1, \dots, X_n, a_1, \dots, a_m) = 0$ יש פיתרון בשלמים חיוביים אם $(a_1, \dots, a_m) \in A$.

דוגמאות: אפשר לומר שמשוואה פולינומיאלית $P_{a_1, \dots, a_m}(x_1, \dots, x_n) = 0$ עם פרמטרים $a_1, \dots, a_m$ מגדירה קבוצת מספרים $A \subset \mathbb{N}^m$ באופן הבא: $(a_1, \dots, a_m) \in A$ אם $P_{a_1, \dots, a_m}(x_1, \dots, x_n) = 0$ יש פיתרון בשלמים חיוביים. למשל:

- המשוואה $a = (x+2)(y+2)$ מגדירה את קבוצת הטבעיים a שאינם ראשוניים.
- המשוואה $a + x = b$ מגדירה את כל הזוגות (a, b) כך ש- $a \leq b$.
- בשיעור על משוואות פל ראינו שהמשוואה $x^2 + ay^2 = 1$ מגדירה את קבוצת המספרים שכוללת את אפס ואת כל המספרים שאינם ריבועים, כלומר $\{0, 2, 3, 5, 6, 7, 8, \dots\}$.

טענה: קבוצה סופית $A \subset \mathbb{N}^m$ היא דיופנטית.

הוכחה: נניח ש- $A = \{(a_1^1, \dots, a_m^1), \dots, (a_1^k, \dots, a_m^k)\}$. נוכיח את הטענה באינדוקציה מלאה על k . אם $k = 1$ אז $A = \{a_1, \dots, a_m\}$ נסתכל על הפולינום

$$P(X, Y_1, \dots, Y_m) = (X^2 + 1)((Y_1 - a_1)^2 + \dots + (Y_m - a_m)^2)$$

מאחר ש- $x^2 + 1 > 0$ לכל x למשוואה $P(X, Y_1, \dots, Y_m) = 0$ יש פיתרון (ובפרט בשלמים חיוביים) אם

$$((Y_1 - a_1)^2 + \dots + (Y_m - a_m)^2) = 0$$

זזה אמ"מ $Y_i = a_i$ לכל $1 \leq i \leq m$. כלומר למשוואה $P(X, Y_1, \dots, Y_m) = 0$ יש פיתרון בשלמים חיוביים אמ"מ $(Y_1, \dots, Y_m) = (a_1, \dots, a_m) \in A = \{(a_1, \dots, a_m)\}$.

כעת נניח שהטענה נכונה לכל $l < k$ ונסתכל על $A = \{(a_1^1, \dots, a_m^1), \dots, (a_1^k, \dots, a_m^k)\}$. נסמן $A_1 = \{(a_1^1, \dots, a_m^1), \dots, (a_1^{k-1}, \dots, a_m^{k-1})\}$ ו- $A_2 = \{(a_1^k, \dots, a_m^k)\}$. אלה קבוצות זרות והגודל שלהן קטן מ- k . לכן לפי הנחת האינדוקציה קיימים פולינומים $P_1(X_1, \dots, X_{n_1}, Y_1, \dots, Y_m)$ ו- $P_2(X_1, \dots, X_{n_2}, Y_1, \dots, Y_m)$ כך שלמשוואות $\{P_i(X_1, \dots, X_{n_i}, a_1, \dots, a_m) = 0\}$ יש פיתרון בשלמים חיוביים אמ"מ $(a_1, \dots, a_m) \in A_i$. נסתכל על הפולינום

$$P(X_1, \dots, X_{\max(n_1, n_2)}, Y_1, \dots, Y_m) = P_1(X_1, \dots, X_{n_1}, Y_1, \dots, Y_m) P_2(X_1, \dots, X_{n_2}, Y_1, \dots, Y_m)$$

בוודאי המקדמים שלו שלמים שהרי המקדמים של P_i שלמים. מאחר שאין מחלקי אפס, למשוואה

$$P(X_1, \dots, X_{\max(n_1, n_2)}, a_1, \dots, a_m) = 0$$

יש פיתרון אמ"מ יש פיתרון לאחת המשוואות $P_i(X_1, \dots, X_{n_i}, a_1, \dots, a_m) = 0$ וזה קורה אמ"מ $(a_1, \dots, a_m) \in A$ ולכן סיימנו.



הגדרה: קבוצה $X \subset \mathbb{N}^m$ היא **רקורסיבית** (או **כריעה**) אם קיים אלגוריתם אשר בהינתן קלט x , עוצר בזמן סופי ומכריז אם הקלט בקבוצה או לא.

הגדרה: קבוצה $X \subset \mathbb{N}^m$ היא **ניתנת למנייה רקורסיבית**¹ (להלן נל"ר) אם קיים אלגוריתם אשר בהינתן קלט x , אם $x \in X$ עוצר בזמן סופי ומכריז ש- x בקבוצה ואחרת לא עוצר לעולם.

דוגמה (בעיית העצירה): ברור שקבוצה רקורסיבית היא נל"ר משום שתמיד אפשר לגרום לאלגוריתם להיכנס ללולאה אינסופית אם קלט כלשהו לא אמור להתקבל. השאלה המעניינת היא האם גם הכיוון ההפוך הוא נכון.

האמת היא שההגדרות הנ"ל טובות לא רק למספרים טבעיים אלא גם לקבוצות אחרות. כעת, נראה שיש קבוצה שהיא נל"ר אך לא רקורסיבית. נשאל האם קיים אלגוריתם אשר בהינתן תוכנית מחשב וקלט מסויים קובע בזמן סופי אם התוכנית תעצור בזמן סופי על הקלט או לא. כלומר, אנחנו שואלים האם הקבוצה

$$\{(P, x) : P \text{ is a program and } x \text{ is an input for which } P \text{ terminates in a finite time}\}$$

היא כריעה או לא. בוודאי הקבוצה נל"ר שהרי אפשר פשוט להריץ את התכנית על הקלט. אם היא עוצרת נכריז שהתוכנית עם הקלט הם בקבוצה ואחרת התכנית תמשיך לרוץ לנצח וגם האלגוריתם שלנו לא יעצור. יותר מעניין להראות שקבוצה זו לא כריעה. נסמן ב- $|P(x)|$ את מספר הפקודות שתוכנית P מבצעת על קלט x . נניח בשלילה שהקבוצה הייתה כריעה והיה לנו אלגוריתם $S(P, x)$ אשר בהינתן תכנית P וקלט כלשהו x פועל באופן הבא:

$$S(P, x) = \begin{cases} 1 & |P(x)| < \infty \\ 0 & |P(x)| = \infty \end{cases}$$

¹ Recursively enumerable

עכשיו נגדיר אלגוריתם $D(P, x)$ באופן הבא:

$$D(P) = \begin{cases} 1 & S(P, P) = 0 \\ \text{infinite loop} & S(P, P) = 1 \end{cases} = \begin{cases} 1 & |P(P)| = \infty \\ 0 & |P(P)| < \infty \end{cases}$$

כלומר D בודק אם P עוצרת על P . אם כן, הוא נכנס ללולאה אינסופית ואם לא הוא מחזיר 1. זה כמובן אפשרי משום שהנחנו ש- S עוצר על כל קלט.

כעת נסתכל על $D(D)$. אם D עוצרת לרוץ על עצמה התכנית נכנסת ללולאה אינסופית ואם D לא עוצרת לרוץ על עצמה אז התכנית עוצרת. אבל זו סתירה. לכן לא יכול להיות שהקבוצה

$\{(P, x): P \text{ is a program and } x \text{ is an input for which } P \text{ terminates in a finite time}\}$

היא רקורסיבית.

טענה: קבוצה דיופנטית $A \subset \mathbb{N}^m$ היא נל"ר.

הוכחה: קיים פולינום P במשתנים $X_1, \dots, X_n, Y_1, \dots, Y_m$ במקדמים שלמים כך שלמשוואה $P(X_1, \dots, X_n, a_1, \dots, a_m) = 0$ יש פיתרון בשלמים חיוביים אם $(a_1, \dots, a_m) \in A$. בהינתן קלט $(a_1, \dots, a_m)$ האלגוריתם יעבור על כל ה- m יות $(x_1, \dots, x_n)$ בסדר מילוני עולה החל מ- $(0, \dots, 0)$ וידפיס את $(a_1, \dots, a_m)$ אם $P(X_1, \dots, X_n, a_1, \dots, a_m) = 0$. ברור שאלגוריתם זה עונה על הדרישות.

☺

משפט (מתיאסביץ' (Matiyasevich) (1970): כל קבוצה נל"ר היא דיופנטית. (לא נוכיח זאת במסגרת זו)

מסקנה: לבעיה העשירית של הילברט אין פיתרון.

הוכחה: הבעיה העשירית של הילברט היא למעשה להוכיח שהשאלה אם לפולינום יש פיתרון טבעי היא כריעה. ידוע שיש קבוצה A שהיא נל"ר אך לא כריעה. קבוצה זו היא דיופנטית. כלומר קיים פולינום P במשתנים $X_1, \dots, X_n, Y_1, \dots, Y_m$ במקדמים שלמים כך שלמשוואה $P(X_1, \dots, X_n, a_1, \dots, a_m) = 0$ יש פיתרון בשלמים חיוביים אם $(a_1, \dots, a_m) \in A$. כעת, אם נניח בשלילה שהשאלה אם יש למשוואה $P(X_1, \dots, X_n, a_1, \dots, a_m) = 0$ פיתרון בטבעיים או לא היא כריעה. אם כך אז גם השאלה אם $(a_1, \dots, a_m) \in A$ או לא היא כריעה. אבל זו סתירה. לכן לא יכול להיות אלגוריתם כללי שמקבל פולינום וקובע אם יש לו פיתרון בשלמים חיוביים או לא.

☺

משפט (פוטנם 1960): תהי קבוצה $A \subset \mathbb{N}$ דיופנטית. אזי קיים פולינום במקדמים שלמים $Q(X_1, \dots, X_k, Y)$ כך ש- A היא קבוצת הערכים השלמים החיוביים המתקבלים ב- $Q(\mathbb{N}, \dots, \mathbb{N}, \mathbb{N})$.

הוכחה: אם A דיופנטית קיים פולינום $P \in \mathbb{Z}[X_1, \dots, X_n, Y]$ כך שלמשוואה $P(X_1, \dots, X_n, a) = 0$ יש פיתרון בשלמים חיוביים אם $a \in A$. נגדיר פולינום חדש

$$Q(X_1, \dots, X_n, Y) = Y(1 - P^2(X_1, \dots, X_n, Y))$$

נטען כעת ש- $A = \mathbb{N} \cap Q(\mathbb{N}, \dots, \mathbb{N}, \mathbb{N})$.

(צ) נניח ש- $a \in A$. אז קיימים $x_1, \dots, x_n \in \mathbb{N}$ כך ש- $P(x_1, \dots, x_n, a) = 0$, לכן

$$Q(x_1, \dots, x_n, a) = a(1 - 0) = a \cdot 1 = a \in A$$

ולכן $A \subset \mathbb{N} \cap Q(\mathbb{N}, \dots, \mathbb{N}, \mathbb{N})$.

(כ) נניח ש- $a \in \mathbb{N} \cap Q(\mathbb{N}, \dots, \mathbb{N}, \mathbb{N})$. נשים לב ש- $Q(X_1, \dots, X_n, a)$ חיובי אמ"מ $1 - P^2(X_1, \dots, X_n, a) > 0$ וזה קורה אמ"מ $1 > P^2(X_1, \dots, X_n, a)$ ומאחר שלכל $X_1, \dots, X_n \in \mathbb{N}$ נובע ש- $P^2(X_1, \dots, X_n, a) \geq 0$ ולכן $a \in A$.



דוגמה: זה אמנם מפתיע משהו אך תוצאה ממשפט פוטנר היא שקיים פולינום שערכיו החיוביים הם בדיוק המספרים הראשוניים, שהרי בוודאי קבוצת הראשוניים היא נל"ר. אלגוריתם ישיר לבדיקת ראשוניות פשוט יבדוק אם המספרים שקטנים מהקלט ושונים מ-1 מחלקים אותו ללא שארית. אם כן סימן שהמספר אינו ראשוני ולכן האלגוריתם ייכנס ללולאה אינסופית. אחרת, המספר ראשוני. ג'ונס (Jones), סאטו (Sato), וואדה (Wada) וווינס (Wiens) עשו את החישובים ו- $k + 2$ הוא ראשוני אמ"מ למשוואות הבאות ב-26 נעלמים יש פיתרון שלם חיובי:

$$\begin{aligned} wz + h + j - q &= 0 \\ (gk + 2g + k + 1)(h + j) + h - z &= 0 \\ 16(k + 1)^3(k + 2)(n + 1)^2 + 1 - f^2 &= 0 \\ 2n + p + q + z - e &= 0 \\ e^3(e + 2)(a + 1)^2 + 1 - o^2 &= 0 \\ (a^2 - 1)y^2 + 1 - x^2 &= 0 \\ 16r^2y^4(a^2 - 1) + 1 - u^2 &= 0 \\ n + l + v - y &= 0 \\ (a^2 - 1)l^2 + 1 - m^2 &= 0 \\ ai + k + 1 - l - i &= 0 \\ \left((a + u^2(u^2 - a))^2 - 1 \right) (n + 4dy)^2 + 1 - (x + cu)^2 &= 0 \\ p + l(a - n - 1) + b(2an + 2a - n^2 - 2n - 2) - m &= 0 \\ q + y(a - p - 1) + s(2ap + 2a - p^2 - 2p - 2) - x &= 0 \\ z + pl(a - p) + t(2ap - p^2 - 1) - pm &= 0 \end{aligned}$$

לא ידוע מהו מספר המשתנים המינימלי ומהי הדרגה המינימלית של פולינום שמגדיר את המספרים הראשוניים.

השערת abc

הגדרה: יהי $n \in \mathbb{N}$. נגדיר את הרדיקל² (או גרעין חופשי מריבועים³) של n ע"י $R(n) = \prod_{p|n} p$ מכפלת הגורמים הראשונים השונים של n .

² Radical
³ Squarefree kernel

השערת-abc (אוסטרלה (Oesterlé) 1985): יהיו $a, b, c \in \mathbb{Z}$ זרים כך ש- $a + b = c$. אזי לכל $\varepsilon > 0$ קיים $C(\varepsilon)$ סופי וקבוע שתלוי רק ב- ε כך ש-

$$\max\{|a|, |b|, |c|\} < C(\varepsilon)R(abc)^{1+\varepsilon}$$

המשמעות של ההשערה הוא היא למעשה שבמידה מסויימת הרדיקל שואף לאינסוף תחת התנאים ש- $a, b, c \in \mathbb{Z}$ זרים כך ש- $a + b = c$. הרי יכול להיות מספר מאוד גדול שהרדיקל שלו הוא קטן, למשל לכל $n \in \mathbb{N}$ $R(2^n) = 2$ ולמרות ש- $\lim_{n \rightarrow \infty} 2^n = \infty$ הרדיקל תמיד $R(2^n) = 2$. אבל מדובר בשלוש מספרים זרים לא חסומות אז גם הרדיקל לא חסום.

דוגמה: נדגים את החשיבות של ε בהשערה. נסתכל על $a_n + b_n = 3^{2^n} - 1 = c_n$. קל לראות באינדוקציה ש- $(3^{2^n} - 1) | 2^n$ לכל n : בוודאי $2^2 = 4 | 80 = 3^{2^2} - 1$. נניח עבור n ואז

$$\begin{aligned} 3^{2^{n+1}} - 1 &= 3^{2^n \cdot 2} - 1 \\ &= (3^{2^n})^2 - 1 \\ &= (3^{2^n} - 1)(3^{2^n} + 1) \end{aligned}$$

ולפי הנחת האינדוקציה זה מתחלק ב- 2^n .

נניח בשלילה שקיים μ כך ש- $c_n \leq \mu \cdot R(a_n b_n c_n)$. אזי

$$\begin{aligned} \max\{|a_n|, |b_n|, |c_n|\} &= 3^{2^n} \\ &\leq \mu \cdot R(a_n b_n c_n) \\ &= \mu \cdot R\left((3^{2^n} - 1) \cdot 1 \cdot 3^{2^n}\right) \\ &= \mu \cdot 3 \cdot R(3^{2^n} - 1) \\ &= \mu \cdot 3 \cdot 2 \cdot R\left(\frac{3^{2^n} - 1}{2^n}\right) \\ &\leq \mu \cdot 3 \cdot 2 \cdot \left(\frac{3^{2^n} - 1}{2^n}\right) \end{aligned}$$

נכפול את שני האגפים ב- $\frac{2^n}{3^{2^n}}$ ונקבל $2^n \leq \mu \cdot 6 \cdot \frac{3^{2^n}-1}{3^{2^n}}$ אבל $6\mu \cdot \frac{3^{2^n}-1}{3^{2^n}} = \lim_{n \rightarrow \infty} \mu \cdot 6 \cdot \frac{3^{2^n}-1}{3^{2^n}}$ ולכן קיבלנו סתירה.

abc-1 LLL

הגדרה: יהיו $a, b, c \in \mathbb{Z}$, $0 \neq a, b, c$. נגדיר את **העצמה**⁴ של השלשה a, b, c להיות

$$P(a, b, c) = \frac{\log \max\{|a|, |b|, |c|\}}{\log R(abc)}$$

השערת abc (מאסר (Masser)): לכל ממשי $\xi > 1$ קיים רק מספר סופי של שלשות של מספרים שלמים זרים a, b, c כך ש- $a + b = c$ וכן $P(a, b, c) > \xi$.

שלשות של שלמים a, b, c אשר מקיימים את התנאי הנ"ל עם $\xi = 1$ נקראות **שלשות- abc** . שלשות שעבורן $P(a, b, c) > 1.4$ נקראות **טובות**.

תרגיל: שתי ההגדרות שקולות.

דוגמה: שתי הדוגמאות לשלשות- abc עם העצמות הכי גדולות הידועות נכון לשנת 2004:

- רייסט (Reyssat): $a = 2, b = 3^{10} \cdot 109, c = 23^5$

$$P(a, b, c) = \frac{\log \max\{2, 3^{10} \cdot 109, 23^5\}}{\log R(2 \cdot 3^{10} \cdot 109 \cdot 23^5)} = \frac{\log 23^5}{\log(2 \cdot 3 \cdot 109 \cdot 23)} = 1.6299$$

- ניט' (Nitaj): $a = 13 \cdot 19^6, b = 2^{30} \cdot 5, c = 3^{13} \cdot 11^2 \cdot 31$

$$P(a, b, c) = \frac{\log \max\{13 \cdot 19^6, 2^{30} \cdot 5, 3^{13} \cdot 11^2 \cdot 31\}}{\log R(13 \cdot 19^6 \cdot 2^{30} \cdot 5 \cdot 3^{13} \cdot 11^2 \cdot 31)} = \frac{\log 3^{13} \cdot 11^2 \cdot 31}{\log(13 \cdot 19 \cdot 2 \cdot 5 \cdot 3 \cdot 11 \cdot 31)} = 1.527$$

תזכורת:

1. יהיו $z_1, \dots, z_r$ וקטורים בלתי תלויים לינארית ב- $\mathbb{R}^n$. **הסריג** Λ עם בסיס $z_1, \dots, z_r$ הוא הקבוצה $\Lambda = z_1\mathbb{Z} + \dots + z_r\mathbb{Z} = \{m_1 z_1 + \dots + m_r z_r : (m_1, \dots, m_r) \in \mathbb{Z}^r\}$.
2. **בסיס מצומצם**⁶ לסריג Λ הוא בסיס $\{z_1, \dots, z_r\}$ כך ש- z_1 הוא וקטור קצר ביותר ב- Λ ולכל $1 < i \leq r$ הוא וקטור קצר ביותר ב- Λ אשר בלתי תלוי לינארית ב- $z_1, \dots, z_{i-1}$.
3. אלגוריתם LLL מחשב בסיס $\{z_1^*, \dots, z_r^*\}$ כמעט מצומצם לסריג. הבסיס כמעט מצומצם במובן הבא: קיימים חסמים $c_1, \dots, c_r$ כך ש- $z_i^* < c_i z_i$ לכל $1 \leq i \leq r$ כאשר $\{z_1, \dots, z_r\}$ בסיס מצומצם של השריג.

דוקצ'יסטר (Dokchister) הציע להשתמש באלגוריתם LLL למציאת שלשות- abc טובות. ניקח מספרים ראשוניים קטנים p_1, p_2, p_3 ונעלה אותם בחזקות גבוהות אך קרובות k_1, k_2, k_3 כדי לקבל את

$$a_0 = p_1^{k_1}, b_0 = p_2^{k_2}, c_0 = p_3^{k_3}$$

בעזרת אלגוריתם LLL ניתן למצוא מקדמים יחסית קטנים α, β, γ כך ש- $\alpha a_0 + \beta b_0 + \gamma c_0 = 0$. אז למספרים $a = \alpha a_0, b = \beta b_0, c = -\gamma c_0$ יש רדיקל קטן ויש להם פוטנציאל להיות בעלי עצמה גבוהה. כמובן, לכל שלשת מספרים גדולים עם רדיקל קטן יש פוטנציאל להיות שלשת- abc טובה, אלא שפרקטית התברר שבשיטה הנ"ל דוקצ'יסטר הצליח למצוא 145 מתוך 154 השלשות- abc הטובות הידועות באותו זמן. בסוף שבוע אחד שבו הריצו חישובים על 30 מחשבים נמצאו 145 מתוך 154 השלשות הידועות עד אז ועוד דוגמאות רבות חדשות.

דוגמה: נסתכל על $a_0 = 1, b_0 = 3^4, c_0 = 5^4$. אנחנו מעוניינים בפתרון המשוואה

$$\alpha + 3^4 \beta + 5^4 \gamma = 0$$

אם (α, β, γ) פיתרון אז $\alpha = 3^4(-\beta) + 5^4(-\gamma)$ ולכן קבוצת הפתרונות ניתנת ע"י

⁵ Lattice
⁶ Reduced basis

$$\Lambda = \begin{pmatrix} 3^4 \\ -1 \\ 0 \end{pmatrix} \mathbb{Z} + \begin{pmatrix} 5^4 \\ 0 \\ -1 \end{pmatrix} \mathbb{Z} = \left\{ \begin{pmatrix} 3^4\beta + 5^4\gamma \\ -\beta \\ -\gamma \end{pmatrix} : \beta, \gamma \in \mathbb{Z} \right\}$$

אלגוריתם LLL נותן לנו במקרה זה את הבסיס הכמעט מצומצם $\left\{ \begin{pmatrix} 23 \\ -8 \\ 1 \end{pmatrix}, \begin{pmatrix} 12 \\ 23 \\ -3 \end{pmatrix} \right\}$ ועכשיו הפיתרונות שאנחנו מחפשים מתקבלים ע"י צירופים לינאריים קטנים של הבסיס. למשל,

$$\begin{aligned} \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} &= 1 \cdot \begin{pmatrix} 23 \\ -8 \\ 1 \end{pmatrix} + 0 \cdot \begin{pmatrix} 12 \\ 23 \\ -3 \end{pmatrix} \Rightarrow P(a, b, c) = 0.9904 \\ \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} &= 1 \cdot \begin{pmatrix} 23 \\ -8 \\ 1 \end{pmatrix} + 1 \cdot \begin{pmatrix} 12 \\ 23 \\ -3 \end{pmatrix} \Rightarrow P(a, b, c) = 0.3336 \\ \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} &= -1 \cdot \begin{pmatrix} 23 \\ -8 \\ 1 \end{pmatrix} + 2 \cdot \begin{pmatrix} 12 \\ 23 \\ -3 \end{pmatrix} \Rightarrow P(a, b, c) = 1.568 \\ \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} &= 4 \cdot \begin{pmatrix} 23 \\ -8 \\ 1 \end{pmatrix} - 1 \cdot \begin{pmatrix} 12 \\ 23 \\ -3 \end{pmatrix} \Rightarrow P(a, b, c) = 1.0848 \end{aligned}$$

אז אנחנו רואים שאחרי חיפוש קצר מצאנו שלש- abc טובה. לפי דוקציסטר ניסויים מראים שכדאי לבדוק את הצירופים הלינאריים של הבסיס אשר ממזערים את אחד הרכיבים. כמו כן, נראה שהשיטה עובדת הכי טוב על מספרים באותו סדר גודל.

הלמה של סיגל (Siegel): נסתכל על המשוואה $a_1x_1 + \dots + a_nx_n = 0$ כאשר המקדמים רציונליים ולא כולם 0 וחסומים ע"י B . למשוואה יש פיתרון רציונלי לא טריוויאלי $(x_1, \dots, x_n)$ כך שלכל $1 \leq i \leq n$ מתקיים $x_i < 1 + (nB)^{\frac{1}{n-1}}$ (לא נוכיח זאת במסגרת זו)

ננתח את השיטה. נניח ש- $a_0 = p_1^{k_1}, b_0 = p_2^{k_2}, c_0 = p_3^{k_3}$ כמו למעלה כולם בערך בגודל N . אז במקרה הכי גרוע בצירוף הלינארי הכי קטן מהצורה $\alpha a_0 + \beta b_0 + \gamma c_0 = 0$ המקדמים הם מסדר גודל $1 + (3N)^{\frac{1}{3-1}} = 1 + \sqrt{3N} \approx \sqrt{3N}$. יש בערך $(\sqrt{3N})^3$ צירופים מהצורה $ia_0 + jb_0 + kc_0$ כאשר $0 \leq i, j, k \leq \sqrt{3N}$. הם כולם בגודל לכל היותר $3N\sqrt{3N} = (\sqrt{3N})^3$ ולכן לפי עיקרון שובר היונים לפחות שניים מהם שווים וההפרש ביניהם נותן את היחס הרצוי⁷. אז במקרה הכי גרוע העצמה של השלשה a, b, c שמתקבלת תהיה:

$$\begin{aligned} P(a, b, c) &\approx \frac{\log(N\sqrt{3N})}{3 \log \sqrt{3N} + \log p_1 + \log p_2 + \log p_3} \\ &= \frac{\log N + \frac{1}{2} \log 3 + \frac{1}{2} \log N}{3 \cdot \frac{1}{2} \log 3 + 3 \cdot \frac{1}{2} \log N + \log p_1 + \log p_2 + \log p_3} \\ &= \frac{2 \log N + \log 3 + \log N}{3 \log 3 + 3 \log N + 2(\log p_1 + \log p_2 + \log p_3)} \end{aligned}$$

⁷ למעשה באופן פורמאלי לא בטוח ניתן להשתמש כאן בעיקרון שובר היונים משום שהיחידים מקורבים ומתקיים שגודל המספר הוא בערך לכל היותר מספר הצירופים. אולי יותר משכנע כאן הטיעון של פרדוקס יום ההולדת. אנחנו לא באמת חייבים 366 אנשים שונים כדי למצוא שניים שיום הולדתם חל באותו יום בשנה...

$$= \frac{3 \log N + \text{constant}}{3 \log N + \text{constant}} \xrightarrow{N \rightarrow \infty} 1$$

זוה החסם של השערת-abc.

השערת ארדש-וודס

השערת ארדש-וודס (Erdős-Woods): קיים שלם k כך שעבור טבעיים m ו- n התנאים

$$0 \leq i \leq k-1 \quad R(m+i) = R(n+i)$$

גוררים $m = n$.

דוגמה: $k = 2$ אינו מתאים להשערת ארדש-וודס משום ש- $1215 = 3^5 \cdot 5$, $75 = 3 \cdot 5^2$ וגם $1216 = 2^6 \cdot 19$, $76 = 2^2 \cdot 19$.

ניתן למצוא אינסוף דוגמאות כאלה. אבל זה כמובן לא אומר שההשערה היא לא נכונה. למעשה, מאמינים ש- $k = 3$ מקיים את הדרוש.

משפט: נניח שהשערת-abc נכונה. אזי השערת ארדש-וודס נכונה עבור $k = 3$ למעט אולי מספר סופי של יוצאי דופן.

הוכחה: צריך להראות שבהינתן טבעיים m ו- n אם $R(m) = R(n)$, $R(m+1) = R(n+1)$ ו- $R(m+2) = R(n+2)$ אז $m = n$ למעט מספר סופי של יוצאי דופן.

נניח בשלילה ש- $m \neq n$. בה"כ $m > n$. נראה שיש לכל היותר מספר סופי של m -ים שעבורם מתקיימת השערת ארדש-וודס עם $k = 3$ וזה יוכיח את הטענה.

נסתכל על $a = m(m+2)$, $b = 1$, $c = (m+1)^2$. אז $a + b = c$ והם זרים. לכן לפי השערת-abc לכל $0 < \varepsilon$ קיים קבוע $C(\varepsilon)$ כך ש-

$$(m+1)^2 \leq C(\varepsilon)R(m(m+2)(m+1)^2)^{1+\varepsilon} = C(\varepsilon)R(m(m+1)(m+2))^{1+\varepsilon}$$

נתון שמתקיים $R(m) = R(n)$, $R(m+1) = R(n+1)$ ו- $R(m+2) = R(n+2)$. לכן עבור $0 \leq i \leq 2$ מתקיים $0 \leq i \leq 2$ $m - n = (m+i) - (n+i) \equiv 0 \pmod{R(m+i)}$. מספרים עוקבים הם תמיד זרים ולכן המחלק המשותף המקסימלי של כל שניים מתוך $R(m)$, $R(m+1)$, $R(m+2)$ הוא 1 או 2. מכאן ש- $|2(m-n)| \leq R(m(m+1)(m+2))$. נובע ש-

$$\begin{aligned} m^2 &\leq (m+1)^2 \\ &\leq C(\varepsilon)R(m(m+2)(m+1)^2)^{1+\varepsilon} \\ &= C(\varepsilon)R(m(m+1)(m+2))^{1+\varepsilon} \\ &\leq C(\varepsilon)(2m-2n)^{1+\varepsilon} \\ &\leq C(\varepsilon)(2m)^{1+\varepsilon} \end{aligned}$$

ומכאן אפשר לקבל חסם ל- m שהרי מאחר ש- $0 < m \leq C(\varepsilon)2^{1+\varepsilon}m^\varepsilon$, כלומר $m^{1-\varepsilon} \leq C(\varepsilon)2^{1+\varepsilon}$ ולבסוף $m \leq (C(\varepsilon)2^{1+\varepsilon})^{\frac{1}{1-\varepsilon}}$.

כלומר יש מספר סופי של m -ים אשר שונים מ- n ועבורם מתקיימת השערת ארדש-וודס עם $k = 3$.



פרמה, קטלן וחברים

הבעיה העשירית של הילברט היא אמנם לא פתירה אבל לא נואשנו מלחפש פיתרון לבעיות דומות תחת אילוצים מגבילים כלשהם.

משפט: נניח שהשערת-abc נכונה. עבור n מספיק גדול אין פתרון לא טריוויאלי למשוואת פרמה $x^n + y^n = z^n$.

הוכחה: נניח ש- $x^n + y^n = z^n$. בה"כ x, y, z זרים. אחרת ניתן לחלק את כל המשוואה ב- $\gcd(x, y, z)^n$. כמו כן ניתן להניח ש- x, y, z חיוביים. נסמן $a = x^n, b = y^n, c = z^n$. אז הם זרים ומתקיים $a + b = c$ ולכן ניתן להשתמש בהשערת-abc. לכל $0 < \varepsilon$ קיים קבוע $C(\varepsilon)$ כך ש-

$$z^n = \max\{x^n, y^n, z^n\} \leq C(\varepsilon)R(x^n y^n z^n)^{1+\varepsilon} = C(\varepsilon)R(xyz)^{1+\varepsilon} \leq C(\varepsilon)(xyz)^{1+\varepsilon}$$

ומכאן ש- $(xyz)^n \leq z^{3n} \leq C(\varepsilon)^3 (xyz)^{3+3\varepsilon}$, כלומר $(xyz)^{n-3-3\varepsilon} \leq C(\varepsilon)^3$ ולכן

$$(n - 3 - 3\varepsilon) \log(xyz) \leq 3 \log C(\varepsilon)$$

אבל $xyz \geq 2$ ולכן $(n - 3 - 3\varepsilon) \log 2 \leq 3 \log C(\varepsilon)$ ולבסוף $n \leq \frac{3 \log C(\varepsilon)}{\log 2} + 3 + 3\varepsilon$. אז עבור n אשר גדול מחסם זה לא קיימים פתרונות לא טריוויאליים למשוואת פרמה וסיימנו.



דוגמה: מעניין לשים לב שהחזקה ומספר המשתנים מהווים גורמים קריטיים בבדיקת קיום הפתרונות. למשל למשוואה $x^3 + y^3 + z^3 + w^3 = 0$ יש אינסוף פתרונות שלמים (לא נוכיח במסגרת זו).

הגדרה: משוואת קטלן (Catalan) היא משוואה מהצורה $x^p - y^q = 1$ כאשר p, q, x, y משתנים ומחפשים פתרונות $2 \leq p, q, x, y \in \mathbb{Z}$.

המקרה ש- $p = q = 2$ במשוואת קטלן הוא לא מעניין כי אז המשוואה היא למעשה

$$x^2 - y^2 = (x - y)(x + y) = 1$$

אבל אנחנו מדברים על חוג השלמים אז $x - y$ ו- $x + y$ הם ההופכיים אחד של השני. האיברים ההפכים היחידים בחוג השלמים הם ± 1 . אז צריך לפתור את המשוואות:

$$\begin{cases} x - y = 1 \\ x + y = 1 \end{cases} \quad \begin{cases} x - y = -1 \\ x + y = -1 \end{cases}$$

במקרה הראשון נקבל $x = -1, y = 0$ ובמקרה השני נקבל $x = 1, y = 0$. אבל אלה לא עומדים בדרישות שהמשתנים יהיו לכל הפחות ≥ 2 ...

אם $2 < p = q$ אז למשוואה יש מספר סופי של פתרונות, שהרי $x^p - q^p = (x - y)Q(x, y)$ כאשר $Q(x, y)$ פולינום מדרגה $p - 1$. כעת, $x^p - y^p = 1$ אמ"מ $x - y = \pm 1$ וכן $Q(x, y) = \pm 1$ עם סימנים מתאימים. מהמשוואה הראשונה נקבל למשל $y = x - 1$ ואז $Q(x, y) = Q(x, x - 1)$ פולינום ב- x ולמשוואה $Q(x, x - 1) = 1$ יש מספר סופי של פתרונות. כל פיתרון כזה קובע את y המתאים לו. ובאותו אופן במקרה ש- $y = x + 1$. סה"כ מספר הפתרונות סופי (או אפס).

האמת היא שדי ברור שאם $p = q$ ו- $x \neq y$ אז $x^p - y^q \neq 1$. בכל אופן מה שיותר מעניין הוא שאפשר להראות שלמשוואת קטלן עם $2 < p, q$ כלשהם יש לכל היותר מספר סופי של פתרונות.

השערת קטלן (ההשערה הוכחה ע"י מיהיילסקו (Mihăilescu) ב-2002): הפיתרון היחיד למשוואת קטלן הוא $3^2 - 2^3 = 1$.

השערת פרמה-קטלן: למשוואה $x^p + y^q = z^r$ יש רק מספר סופי של פתרונות כאשר $x, y, z \in \mathbb{N}$ זרים ו- $p, q, r \in \mathbb{N}$ כך ש- $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$.

דוגמה: הפתרונות הידועים כיום למשוואת פרמה-קטלן הם:

$$\begin{aligned} 1^p + 2^3 &= 3^2 \\ 2^5 + 7^2 &= 3^4 \\ 13^2 + 7^3 &= 2^9 \\ 2^7 + 17^3 &= 71^2 \\ 3^5 + 11^4 &= 122^2 \\ 33^8 + 1549034^2 &= 15613^2 \\ 1414^3 + 2213459^2 &= 65^7 \\ 9262^3 + 15312283^2 &= 113^7 \\ 17^7 + 76271^3 &= 21063928^2 \\ 43^8 + 96222^3 &= 30042907^2 \end{aligned}$$

משערים שאין כלל פתרונות כאשר כל החזקות גדולות מ-3.

משפט: נניח שהשערת-abc נכונה. אז השערת פרמה-קטלן נכונה.

הוכחה: נסתכל על התנאי $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$. נטען ש- $\frac{41}{42} \leq \frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq 1$, שהרי אם $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$ אז $p \neq 1$. אז p לכל הפחות 2 ואז צריך ש- $\frac{1}{q} + \frac{1}{r} < \frac{1}{2}$. לכן $q \neq \frac{1}{2}$ והוא לכל הפחות 3. לכן $\frac{1}{r} < \frac{1}{6}$ ולכן r לכל הפחות 7. מכאן ש- $\frac{41}{42} = \frac{1}{2} + \frac{1}{3} + \frac{1}{6} \leq \frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq 1$. אז לפי השערת-abc נובע שלכל $0 < \varepsilon$ קיים קבוע $C(\varepsilon)$ כך ש- $\max\{|x|^p, |y|^q, |z|^r\} \leq C(\varepsilon)R(x^p y^q z^r)^{1+\varepsilon}$. בה"כ x, y, z חיוביים ו- z^r הוא המקסימלי. אז מתקיים

$$\begin{aligned} z^r &= \max\{|x|^p, |y|^q, |z|^r\} \\ &\leq C(\varepsilon)R(x^p y^q z^r)^{1+\varepsilon} \\ &= C(\varepsilon)R(xyz)^{1+\varepsilon} \\ &\leq C(\varepsilon)(xyz)^{1+\varepsilon} \\ &= C(\varepsilon) \left((x^p)^{\frac{1}{p}} (y^q)^{\frac{1}{q}} (z^r)^{\frac{1}{r}} \right)^{1+\varepsilon} \end{aligned}$$

$$\leq C(\varepsilon) \left((z^r)^{\frac{1}{p} + \frac{1}{q} + \frac{1}{r}} \right)^{1+\varepsilon}$$

$$\leq C(\varepsilon) \left(z^{\frac{41}{42}r} \right)^{1+\varepsilon}$$

נבחר למשל $\varepsilon = \frac{1}{83}$ ונקבל $z^r < C \left(\frac{1}{83} \right)^{83}$ ולכן z חסום ומהיותו מקסימלי גם x, y חסומים ומספר הפתרונות סופי.

☺

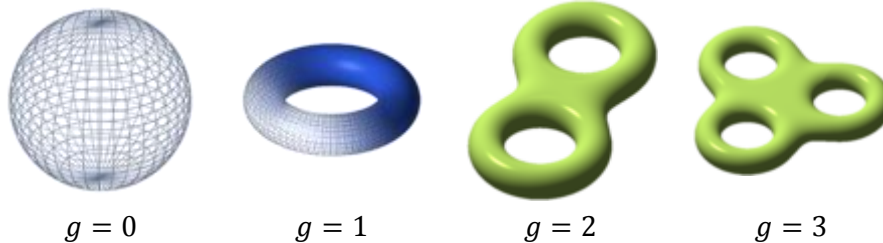
השערת מורדל

הגדרה: יהי $\mathbb{K}$ שדה ותהי $\mathcal{C}$ עקומה שנתונה ע"י משוואה דיופנטית הומוגנית $P(X, Y) = 0$ כאשר P פולינום עם מקדמים ב- $\mathbb{K}$. נקודה (x, y) על העקומה $\mathcal{C}$ נקראת **סינגולרית** אם $\nabla P(x, y) = 0$.⁸
 נקודה סינגולרית (x, y) נקראת **נקודה כפולה רגילה**⁹ אם $\text{rank}(H(P(x, y))) < 2$.¹⁰ אם כל הנקודות הסינגולריות של העקומה הן כפולות רגילות אז הגנוס¹¹ של $\mathcal{C}$ מוגדר ע"י

$$g = \frac{1}{2}(n-1)(n-2) - r$$

כאשר $n = \deg P$ ו- r מספר הנקודות הכפולות הרגילות. אם עקומה היא חלקה, כלומר ללא נקודות סינגולריות, אז $r = 0$.

אפשר להראות שהגנוס הוא למעשה מספר ה"חורים" שיש במשטח.



השערת מורדל (Modell) (ההשערה הוכחה ע"י פלטינגס (Faltings) בשנת 1983): תהי $\mathcal{C}$ עקומה שמוגדרת מעל $\mathbb{Q}$ עם גנוס גדול מ-1. אזי ל- $\mathcal{C}$ יש רק מספר סופי של נקודות רציונליות. (לא נוכיח זאת במסגרת זו)

⁸ הגרדיאנט (Gradient) של פונקציה f הוא $\nabla f(x_1, \dots, x_n)|_{\bar{x}} = \left(\frac{\partial f}{\partial x_1} \Big|_{\bar{x}}, \dots, \frac{\partial f}{\partial x_n} \Big|_{\bar{x}} \right)$

⁹ Ordinary double point

¹⁰ ההסיאן (Hessian) של פונקציה f הוא מטריצת הנגזרות השניות

$$H(f(x_1, \dots, x_n))|_{\bar{x}} = \begin{pmatrix} \frac{\partial^2 f}{\partial x_1 x_1} \Big|_{\bar{x}} & \dots & \frac{\partial^2 f}{\partial x_1 x_n} \Big|_{\bar{x}} \\ \vdots & \ddots & \vdots \\ \frac{\partial^2 f}{\partial x_n x_1} \Big|_{\bar{x}} & \dots & \frac{\partial^2 f}{\partial x_n x_n} \Big|_{\bar{x}} \end{pmatrix}$$

¹¹ Genus

במקרים שהגנוס הוא 0 או 1 טיפלו בשבוע שעבר. אם הגנוס הוא 0 אז למעשה מדובר בספרה ואז שאין נודות רציונליות או שיש אינסוף. ואם הגנוס הוא 1 אז מדובר בעקומה אליפטית ומשפט מורדל אומר שהנקודות הרציונליות מהוות חבורה אבלית נוצרת סופית.

הגדרה: עקומת פרמה היא העקומה $x^n + y^n - 1 = 0$

הערה: נשים לב שכל נקודה רציונלית על עקומת פרמה מתאימה לפיתרון של משוואת פרמה

$$\text{ולחפ. שהרי, } p^n + r^n = (qs)^n \Leftrightarrow \left(\frac{p}{q}\right)^n + \left(\frac{r}{s}\right)^n - 1 = 0$$

טענה: עקומת פרמה היא חלקה.

הוכחה: מתקיים $\nabla(x^n + y^n - 1) = (nx^{n-1}, ny^{n-1})$ אבל $(nx^{n-1}, ny^{n-1}) = (0,0)$ אם $n=1$ או $n=2$ אבל הראשית לא נמצאת על העקומה ולכן אין לעקומת פרמה אף נקודה סינגולרית.



מסקנה: הגנוס של עקומת פרמה הוא $g = \frac{1}{2}(n-1)(n-2)$

אם $n=2$ אז $g=0$ ויש אינסוף פתרונות למשוואה – השלוש הפיתגוריות. אם $n=3$ אז $g=1$ אבל אוילר הוכיח כבר הוכיח שאין פתרונות לא טריוויאליים. אם $n \geq 4$ אז $g > 2$ ואז לפי משפט פלטינגס לעקומת פרמה יש רק מספר סופי של נקודות רציונליות ולכן למשוואת פרמה יש לכל היותר מספר סופי של פתרונות שלמים.

משפט: נניח שהשערת-abc נכונה. אזי השערת מורדל נכונה. (לא נוכיח זאת במסגרת זו)

מקורות נוספים

1. Diophantine sets : <http://www.jstor.org/view/00029890/di991801/99p02593/0>
2. The abc-conjecture : <http://www.msci.memphis.edu/preprint/wthesis.pdf>
3. The abc-conjecture : http://www.thehcmr.org/issue1_1/elkies.pdf
4. LLL & abc: <http://tinyurl.com/2srjh6> (from the university's computers or using tango from home)
5. Siegel's lemma: http://en.wikipedia.org/wiki/Siegel's_lemma

22.1.08

תורה
הוסיפה

הנוכחים וההאים איננו
מכאן טוב לאטמאם
שיעור זה ארץ.

פונקציה $\{0, \pi\}$

$$\sum \frac{1}{n^2} = \frac{\pi^2}{6}$$

$$\int_0^1 \int_0^1 \frac{dx dy}{1-x^2 y^2}$$

הוכחה: (סתם) (ראינו)

האם הפונקציה חסומה אם כן, אולי קצת

הפונקציה $f(x,y)$ וחסומה אם ϵ קטן, אולי קיים δ אחר

$$y = \frac{\sin v}{\cos u}$$

$$x = \frac{\sin u}{\cos v} \quad (1)$$

$$\sin v \leq \cos u = \sin(\frac{\pi}{2} - u)$$

$$\sin u \leq \cos v = \sin(\frac{\pi}{2} - v) \quad \text{אם}$$

$$0 \leq u, v \leq \frac{\pi}{2}$$

$\Leftarrow$

חשוב לא להיחלש

$$\begin{vmatrix} \frac{\partial x}{\partial u} & \frac{\partial x}{\partial v} \\ \frac{\partial y}{\partial u} & \frac{\partial y}{\partial v} \end{vmatrix} = \begin{vmatrix} \frac{\cos u}{\cos v} & \frac{\sin u \sin v}{\cos^2 v} \\ \frac{\sin v \sin u}{\cos^2 u} & \frac{\cos v}{\cos u} \end{vmatrix} = 1 - \tan^2 u \tan^2 v$$

$$\Rightarrow \int_0^{\frac{\pi}{2}} \int_0^{\frac{\pi}{2}} \frac{1 - \tan^2 u \tan^2 v}{1 - \tan^2 u \tan^2 v} du dv =$$

$$\text{area} \left(\begin{matrix} (0, \frac{\pi}{2}) \\ (0,0) \\ (\frac{\pi}{2}, 0) \end{matrix} \right) = \frac{\pi^2}{8}$$

$$p \delta \quad q < 1 \quad \text{אם} \quad \frac{1}{1-q} = \sum_{n=0}^{\infty} q^n \quad (2)$$

$$\begin{aligned} I &= \int_0^1 \int_0^1 \sum_{n=0}^{\infty} (x^2 y^2)^n dx dy = \sum_{n=0}^{\infty} \int_0^1 \int_0^1 x^{2n} y^{2n} dx dy = \\ &= \sum_{n=0}^{\infty} \frac{1}{(2n+1)^2} = \sum_{n=1}^{\infty} \frac{1}{n^2} - \sum_{n=1}^{\infty} \frac{1}{(2n)^2} = (1 - \frac{1}{4}) \sum_{n=1}^{\infty} \frac{1}{n^2} \end{aligned}$$

(11)

באופן קומה $\sum \frac{1}{n^4} = \frac{\pi^4}{90}$
 באופן בלי $\sum \frac{1}{n^{2k}} = B_k \cdot \pi^{2k}$ כאשר $B_k \in \mathbb{Q}$ מספר רציונלי
 (מקדמים באיזו סילור & פונקציה טריגונומטרית - פשוטה)

שאלה פתוחה: ידוע שקיים הגבול
 $\lim_{n \rightarrow \infty} (1 + \frac{1}{2} + \dots + \frac{1}{n} - \log n) = \gamma =$ מספר אويلר
 והאם $\gamma \in \mathbb{Q}$?

הגבול $\sum \frac{1}{n^k} \notin \mathbb{Q}$ (ובעזר k - π טרנסצנדנטי)
 מה ידועי חלקל אצטמיל? $\sum \frac{1}{n^3} = \zeta(3)$ עמל עבור $\zeta(3)$ אין (נסחה)
 יפה כמו הלקרה הציגו וממשל הרבה למן לא ידעו מה קורה
 עמ לה. (גדירחסן בלי) $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ פונקציית זטא של רימן
 $s > 1$

משפט (1978) $\zeta(3) \notin \mathbb{Q}$

פונקציית זטא יש תכונה יפה:
 $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p (1 - p^{-s})^{-1}$
 (הכאן p ראשוני ו- s השני)
 כי זה טור גאומטרי + עמ $q = p^{-s}$

$$\prod_p \left(\sum_{h=0}^{\infty} p^{-hs} \right) = \sum_{\substack{p_1, \dots, p_r \\ \text{שונים}}} p_1^{-s} \dots p_r^{-s} = \sum_{\substack{p_1, \dots, p_r \\ \text{אם זה אצטמילי מספר סבילי}}} (p_1^{n_1} \dots p_r^{n_r})^{-s} = \sum_{n=1}^{\infty} n^{-s}$$

האמר הים שאלו ζ אפשר להקצות גם על המרחבים (הים)
 מתכנסת על $\text{Re}(s) > 1$. רימן ילזה של פונקציה הלאה יש
 המלכה אנליטיק גם מעבר ל- $\text{Re}(s) > 1$. לעולם בגחום
 $0 < \text{Re}(s) < 1$ יש הרבה אפסים לפונקציה! תחום זה
 נקרא הרצועה הקריטית.

השערת רימן (האמרה שלמה) ζ האפסים של פונקציית זטא של רימן
 הרצועה הקריטית נמצאים על הישר הקטע $\text{Re}(s) = \frac{1}{2}$.

משפט הפונקציה של אפסים $\text{Re}(s) = 1$ (לקחה) משפט המעבר הראשוניים.

משפט המספרים הראשונים:

$$\#\{p: p \leq x\} = \pi(x) \sim Li(x) = \int_2^x \frac{dt}{\log t} \left(\sim \frac{x}{\log x} \right)$$

מה זה המשפט?

$$\underbrace{RH_f}_{Res \geq f} \Leftrightarrow |\pi(x) - Li(x)| = o(x^f)$$

כל מה שאפשר יהיה להוכיח בעזרת סים של פונקציות מתחבא.

כל השערה כזו שקולה ל- $|\pi(x) - Li(x)| = o(x^{\frac{1}{2}+\epsilon})$ כל ϵ

כל $f > \frac{1}{2}$ $RH_f \Leftrightarrow RH$

ייתכן ש- $RH_{\frac{1}{2}}$ אכן נכונה אבל RH_f לא $f > 1$.

משפט: $\zeta(3) \notin \mathbb{Q}$

הוכחה: מהסתברות מסוי קשה להגיע למסקנה.

הרעיון: הנסיס הוא לקרב את $\zeta(3)$ עם מספרים רציונליים.

אם $|\alpha - \frac{p}{q}| < \frac{1}{q^{4+\epsilon}}$ עבור אינסוף q אז α איננו רציונלי.

הצמד הסכמי הוא זקן, אם הסדר אולי זה צורך אולי עובד.

Apery אולי פיתח את $\zeta(3)$ (שברים משולבים מובילים).

שבר משולב מוביל הוא שבר שבו המונה והמכנה הם לא תלויים.

$$\frac{\pi}{4} = \frac{1}{1 + \frac{1}{2 + \frac{9}{2 + \dots + \frac{(2n+1)^2}{2 + \dots}}}}$$

האופן שבו מנסים מוביל (הוא)

$$\frac{a_n}{b_n} = \frac{a_1}{b_1 - \frac{A_1 C_1}{b_1 - \frac{A_2 C_2}{b_2 - \dots - \frac{A_{n-1} C_{n-1}}{b_{n-1} - \frac{A_n C_n}{b_n}}}}}$$

הסדרה a_n, b_n מקיימים את (נסתח הריקנסיה)

$$A_n u_{n+1} - B_n u_n + C_n u_{n-1} = 0$$

כאשר $a_n = u_n$ או $b_n = u_n$, ההוכחה פשוטה.

$$\left| \frac{a_n}{b_n} - \frac{a_{n-1}}{b_{n-1}} \right| = \frac{a_n b_{n-1} - a_{n-1} b_n}{b_n b_{n-1}} =: \frac{c_n}{b_n b_{n-1}}$$

$A_n = 1$ נבחר C_n וקווינו a_n, b_n וקווינו c_n

$$c_{n+1} = a_{n+1} b_n - a_n b_{n+1} = (B_n a_n - G_n a_{n-1}) b_n -$$

יש לנו $c_{n+1} = C_n c_n$ ש"כ
אם $A_n = 1$ ש"כ

$$G_{n+1} = \frac{C_n}{A_n} c_n$$

$$- a_n (B_n b_n - G_n b_{n-1}) =$$

$$= G_n (a_{n-1} b_n - a_n b_{n-1}) = G_n c_n$$

$$c_n = 6n^3 \leftarrow \begin{cases} A_n = (n+1)^3 & \text{המקרה } (p \text{ בסבב}) \\ B_n = 34n^2 + 54n^2 + 27n + 5 \\ G_n = n^3 \end{cases}$$

אם A_n, B_n, C_n הם פולינומים של n אז $\zeta(3)$ הוא

$$\zeta(3) = \frac{6}{5 - \frac{1}{117 - \dots - \frac{n^6}{B_n} \dots}} = \lim \frac{a_n}{b_n}$$

המספר a_n, b_n נבחרים כך

$$b_n = \sum_{k=0}^n \binom{n}{k}^2 \binom{n+k}{k}^2$$

$$a_n = \sum_{k=0}^n C_{n,k} \binom{n}{k}^2 \binom{n+k}{k}^2$$

$$C_{n,k} = \sum_{m=1}^n \frac{1}{m^3} + \sum_{m=1}^k \frac{(-1)^{m-1}}{2m^3 \binom{n}{k} \binom{n+m}{m}} \text{ נאם}$$

זכור, a_n, b_n הם מספרים שלמים וחסומים.
ההקדמה, זה הרבה זמן לא נראה.

$$\lim \frac{a_n}{b_n} = \zeta(3) \text{ - ערך מסוים}$$

$$E_{n,k} \leq \frac{1}{n^2} \text{ אפשר לראות - } E_{n,k} = \sum_{m=1}^k \frac{(-1)^{m-1}}{2m^3 \binom{n}{k} \binom{n+m}{m}} \text{ (נסי)$$

$$W_{n,k} = \binom{n}{k}^2 \binom{n+k}{k}^2 \text{ (נסי) } |C_{n,k} - \zeta(3)| \leq \frac{K}{n^2} \leftarrow$$

$$\left| \sum_k C_{n,k} W_{n,k} - \sum_k \zeta(3) W_{n,k} \right| = \sum_k |C_{n,k} - \zeta(3)| W_{n,k} \leq \frac{K}{n^2} \sum_k W_{n,k}$$

(חלק ב) - $W_{n,k}$ ומצויק (קרא) $\epsilon - \frac{k}{n^2} \rightarrow 0$ $|\frac{a_n}{b_n} - \zeta(3)| < \frac{k}{n^2}$
 אסג מה שרצינו.

ואגו אהראל שזה איז ציור δ . נשים אג שלמה אסג
 אס אהצא אסג א קרם הוהתכנס:

$$\left| \frac{a_n}{b_n} - \frac{a_{n+1}}{b_{n+1}} \right| = \frac{cn^3}{b_n b_{n+1}}$$

אצוי $[n] = \{1, \dots, n\}$ - האספר האינואלי אמתה $n, 1, \dots$

אסג $[n]^3 \cdot a_n \in \mathbb{Z}$

אריסוי נוס אהראל $\zeta(3) \notin \mathbb{Q}$

$$\left| \frac{a_n}{b_n} - \zeta(3) \right| = \left| \frac{[n]^3 a_n}{[n]^3 b_n} - \zeta(3) \right| < \frac{1}{([n]^3 b_n)^{1+\delta}}$$

זה מה שרצינו $0 < \delta$ אסג
 הוה אצונו $\lim_{n \rightarrow \infty} \frac{\log [n]^3}{n} \leq 1$ (אסג אסג)
 האספרים האסוניים.

$$k = \beta n \quad n \text{ זקח} \quad b_n = \sum_{k=0}^n \left(\binom{n}{k} \binom{n+k}{k} \right)^2 + 1$$

$$\log \binom{n}{\beta n} \sim n(\beta \log \beta + (1-\beta) \log (1-\beta))$$

$$n f(\beta) = 2 \left(\log \binom{n}{\beta n} + \log \binom{n+\beta n}{\beta n} \right) \quad \text{הוהתנהא אסג}$$

$$\log b_n = n \cdot \max_{\beta} f(\beta) > 3n \quad \text{אסג אסג}$$

$$\left| \frac{[n]^3 a_n}{[n]^3 b_n} - \zeta(3) \right| = \frac{n^3}{b_n b_{n+1}} \quad \text{אסג אסג}$$

$$\log b_n > 3n \quad \text{אסג אסג} \quad \lim_{n \rightarrow \infty} \frac{\log [n]^3}{n} \leq 1$$

$$\frac{\log b_n}{n} \geq (1+\delta) \frac{\log [n]^3}{n}$$

$$\delta = \max f - 3$$



אסג אסג