

תורת המספרים

סיכום הגדרות טענות ומשפטים

אביב 2017

1 פירוק לגורמים ראשוניים

1.1 הגדרות

חוג $A \subseteq \mathbb{C}$ נקראת חוג אם:

- היא מכילה את 0 ואת 1
- סגורה תחת חיבור, חיסור, וכפל

הפיך A חוג. $a \in A$ נקרא הפיך אם $a \neq 0$, $a^{-1} \in A$.
קבוצת כל ההפיכים ב- A תסומן ב- A^* .

חלוקה A חוג. $a, b \in A$.
 a מחלק את b (מסומן $a|b$) אם קיים $c \in A$ כך ש- $ac = b$.

חבר, אי-פריק, וראשוני A חוג. $a, b \in A$.
נאמר ש- b חבר של a אם יש $\varepsilon \in A^*$ כך ש- $b = \varepsilon a$.
 a נקרא אי-פריק אם $a \neq 0$, $a \notin A^*$, וכל מחלק של a הוא חבר של a או הפיך.
 $p \in A$ נקרא ראשוני אם $p \neq 0$, $p \notin A^*$, וגם $p|ab \implies p|a$ or $p|b$.

מחלק משותף $a, b \in \mathbb{Z} \setminus \{0\}$. c נקרא מחלק משותף של a, b אם $c|a$ וגם $c|b$.
אוסף כל המחלקים המשותפים של a, b זו קבוצה סופית. האיבר הגדול ביותר בקבוצה זו נקרא המחלק המשותף הגדול ביותר ומסומן $\gcd(a, b)$.
אם $\gcd(a, b) = 1$ נאמר ש- a, b זרים.

1.2 טענות

תכונות חלוקה A חוג.

- לכל $b \in A$, $\pm 1|b$
- לכל $b \in A$ ולכל $a \in A^*$, $a|b$
- כל איבר מחלק את 0, ו-0 מחלק רק את עצמו.
- אם $a|b$ ו- $b \neq 0$ אז $|a| \leq |b|$.
- אם $a|b$ ו- $b|c$ אז $a|c$.
- אם $a|b$ ו- $c \in A$ אז $ac|bc$.
- אם $a|c$, $a|b$ ו- $u, v \in A$ אז $a|ub + vc$.

טענות על אי-פריקים וראשוניים

טענה יהי A חוג. אם $p \in A$ ראשוני אז p אי פריק.

טענה אם $A = \mathbb{Z}$, אז כל $a \in A, a \neq 0$ שאינו הפיך אפשר לרשום כמכפלה של אי-פריקים.

טענה נניח A חוג, בו כל מזפר חוץ מ-0 והפיכים אפשר לרשום כמכפלה של אי-פריקים. אזי הפירוק הוא יחיד \iff כל אי-פריק ב- A הוא ראשוני.

חלוקה עם שארית נניח $a, b \in \mathbb{Z}, a > 0$. אז יש $q \in \mathbb{Z}, 0 \leq r < a, r \in \mathbb{Z}$ יחידים כך ש: $b = aq + r$. נקראת השארית שמתקבלת מחלוקת a ב- b .

טענה על gcd

טענה לכל $a, b \in \mathbb{Z}$, יש $k, l \in \mathbb{Z}$ כך ש- $gcd(a, b) = ka + lb$.

מסקנה ב- \mathbb{Z} כל אי פריק הוא ראשוני. מכאן גם שכל פירוק לאי-פריקים הוא יחיד.

מסקנה אם $d = gcd(a, b)$ ו- n מחלק משותף של a, b אז $n|d$.

1.3 אלגוריתם אוקלידס

יהי $a, b \in \mathbb{Z}$.

בה"כ $a > 0$. נסמן $a = r_0, b = r_{-1}$. נבצע חלוקה עם שארית:

$$b = q_0 a + r_1 = q_0 r_0 + r_1 \quad 0 \leq r_1 < r_0 = a$$

$$r_0 = q_1 r_1 + r_2 \quad 0 \leq r_2 < r_1$$

ממשיכים כאשר בצעד ה- j :

$$r_{j-1} = q_j r_j + r_{j+1} \quad 0 \leq r_{j+1} < r_j$$

ממשיכים עד שמגיעים לשארית 0. כלומר עד שיש k עבורו $r_{k+1} = 0$.

טענה $gcd(a, b) = r_k$

ניסוח מטריציוני את הנוסחה $r_{j-1} = q_j r_j + r_{j+1}$ ניתן לרשום גם כך:

$$\begin{pmatrix} r_j \\ r_{j+1} \end{pmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q_j \end{bmatrix} \begin{pmatrix} r_{j-1} \\ r_j \end{pmatrix}$$

(מטריצה הפיכה בשלמים).

2 מספרים ראשוניים

2.1 משפטים

מסקנה מהפרק הקודם לכל $n \in \mathbb{N}, n \geq 2$, יש $k \in \mathbb{N}$ ראשוניים שונים p_1, p_2, \dots, p_k ו- r_1, r_2, \dots, r_k כך ש- $n = p_1^{r_1} \cdot \dots \cdot p_k^{r_k}$. פירוק זה יחיד עד כדי שינוי סדר.

משפט אוקלידס יש אינסוף ראשוניים

הגדרה נסמן את הראשוניים בסדר עולה $p_1 < p_2 < \dots < p_k < \dots$
נגדיר את הפונקציה $\Pi(x)$ להיות:

$$\Pi(x) = \#\{k | p_k \leq x\}$$

משפט המספרים הראשוניים (לא הוכח) $\Pi(x) \sim \frac{x}{\log x}$

משפט צ'בישב קיימים קבועים חיוביים c_1, c_2 כך ש- $c_1 \frac{x}{\log x} \leq \Pi(x) \leq c_2 \frac{x}{\log x}$

טענה לכל $l \in \mathbb{N}$, $p_l < 2^{2^l}$

מסקנה לכל $x \geq 2$, $\Pi(x) \geq \log(\log x)$

2.2 שיטות פשוטות למציאת ראשוניים

מספרי פרמה

$$F_n = 2^{2^n} + 1$$

פרמה ניחש שמספרים אלה ראשוניים. למעשה רק ה-4 הראשוניים ראשוניים.

טענה לכל $n \neq m$, $\gcd(F_n, F_m) = 1$.
מסקנה - יש אינסוף מספרים ראשוניים.

מספרי מרסן

$$M_n = 2^{p_n} - 1 \quad p_n \text{ is prime}$$

לא כל מספרי מרסן ראשוניים.

3 פיתרון קונגרוואנציות

3.1 חוג השלמים מודולו m (\mathbb{Z}_m)

יהי m טבעי, $a, b \in \mathbb{Z}$ נקראים קונגרוואנטים מודולו m אם $m | b - a$. בצורה לא פורמלית - אם a, b משאירים את אותה שארית בחלוקה ב- m .

נסמן $a \equiv b \pmod{m}$.

יחס זה הוא יחס שקילות. את קבוצת מחלקות השקילות נסמן ב- \mathbb{Z}_m . לקבוצה זו קוראים השלמים מודולו m .

טענה אפשר לבצע פעולות חיבור, חיסור, וכפל על נציגי המחלקות. לכן \mathbb{Z}_m הוא חוג.

הגדרה איבר $a \in \mathbb{Z}_m$ נקרא הפיך אם יש $b \in \mathbb{Z}_m$ כך ש- $ab \equiv 1 \pmod{m}$. נסמן את קבוצת האיברים ההפיכים ב- \mathbb{Z}_m^* .

טענות

טענה $a \in \mathbb{Z}_m^* \iff \gcd(a, m) = 1$

טענה נניח $\gcd(k, m) = 1, k \in \mathbb{Z}, a, b \in \mathbb{Z}_m$ אזי:

$$a \equiv b \pmod{m} \iff ka \equiv kb \pmod{m}$$

מסקנה \mathbb{Z}_m שדה $\iff m$ ראשוני.

טענה נניח ש- r מחלק משותף של k, m אזי:

$$ka \equiv kb \pmod{m} \iff \frac{k}{r}a \equiv \frac{k}{r}b \pmod{\frac{m}{r}}$$

מסקנה

$$a \equiv b \pmod{\frac{m}{\gcd(m, k)}} \iff ka \equiv kb \pmod{m}$$

קבוצת ההפיכים מודולו m (\mathbb{Z}_m^*)

הגדרה עבור $m \geq 2$ טבעי נסמן $|\mathbb{Z}_m^*| = \phi(m)$

טענה אם $n = p_1^{r_1} \cdot \dots \cdot p_k^{r_k}$ אזי

$$\phi(n) = \prod_{i=1}^k p_i^{r_i-1} (p_i - 1) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)$$

מסקנה ϕ כפלית. כלומר לכל $n, m \in \mathbb{Z}, \gcd(n, m) = 1$ מתקיים $\phi(mn) = \phi(n)\phi(m)$.

טענה לכל n טבעי

$$\sum_{d|n} \phi(d) = n$$

3.2 פיתרון קונגרואנציה ממעלה ראשונה ($ax \equiv b \pmod{m}$) (*)

משפט נסמן ב- $d = \gcd(a, m)$ אז מספר הפתרונות ל- $(*)$ ב- \mathbb{Z}_m הוא:

$$\begin{cases} 0 & d \nmid b \\ d & d|b \end{cases}$$

כמו כן, אם $d|b$ אז מספר הפתרונות ב- $\mathbb{Z}_{m/d}$ הוא 1.

משפט השאריות הסיני נניח $m_1 \cdot \dots \cdot m_k$ זרים בזוגות. יש $x \in \mathbb{Z}$ כך ש- $x \equiv c_i \pmod{m_i}$ (*).
אז אם $y \in \mathbb{Z}$ פיתרון ל- $(*)$ אזי $x \equiv y \pmod{M}$ כאשר $M = \prod_{i=1}^k m_i$.

משפט פרמה הקטן אם p ראשוני ו- $x \not\equiv 0 \pmod{p}$ אז $x^{p-1} \equiv 1 \pmod{p}$.

משפט אוילר יהי $m \in \mathbb{N}$, $m \geq 2$. אז לכל $x \in \mathbb{Z}_m^*$, $x^{\phi(m)} \equiv 1 \pmod{m}$.

משפט וילסון יהי p ראשוני. אז $(p-1)! \equiv -1 \pmod{p}$.

3.3 מבחן הראשוניות של מילר רבין

בהינתן $m \geq 3$ אי זוגי, נרשום $m-1 = 2^l \cdot s$, s אי זוגי. נבחר $b \in \{1, \dots, m-1\}$ ונבצע את הפעולות הבאות:

1. אם $b^{m-1} \not\equiv 1 \pmod{m}$ פולטים m נכשל לפי בסיס b ועוצרים.

2. אם $b^s \equiv 1 \pmod{m}$ פולטים m עבר לפי בסיס b ועוצרים.

3. מוצאים את ה- r היחיד המקיים $b^{2^{r+1} \cdot s} \equiv 1 \pmod{m}$, $b^{2^r \cdot s} \not\equiv 1 \pmod{m}$. אם $x \equiv -1 \pmod{m}$ פולטים m עבר לפי בסיס b ועוצרים. אחרת פולטים m נכשל לפי בסיס b ועוצרים.

משפט אם m ראשוני, אז לכל b , האלגוריתם יסתיים בפלט " m עבר לפי בסיס b ".

משפט אם m לא ראשוני, אזי:

$$|\{b \in \mathbb{Z}_m^* \mid m \text{ passes with } b\}| \leq \frac{1}{4} \phi(m) = \frac{1}{4} |\mathbb{Z}_m^*|$$

3.4 שורשים פרימיטיביים

המספר המינימלי k המקיים $a^k \equiv 1 \pmod{m}$ נקרא הסדר של a מודולו m ומסומן $\text{ord}_m(a)$. a נקרא שורש פרימיטיבי מודולו m אם $\text{ord}_m(a) = \phi(m)$.

משפטים וטענות

טענה אם $a^r \equiv 1 \pmod{m}$ ו- $k = \text{ord}_m(a)$ אז $k \mid r$.

מסקנה $\text{ord}_m(a) \mid \phi(m)$

טענה אם a פרימיטיבי מודולו m אז $\mathbb{Z}_m^* = \{1, a, a^2, \dots, a^{\phi(m)-1}\}$

משפט האיבר הפרימיטיבי אם m ראשוני אז קיים איבר פרימיטיבי מודולו m .

משפט קיים איבר פרימיטיבי מודולו $m \iff m = 2, m = 4, m = p^k, m = 2p^k$ (כאשר p ראשוני אי זוגי)

3.5 ההעתקה $x \mapsto x^r \pmod{m}$ (העלאה בחזקת r)

נגדיר את ההעתקה $f: \mathbb{Z}_m^* \rightarrow \mathbb{Z}_m^*$ ע"י $f(x) = x^r \pmod{m}$.

טענות

טענה נניח שקיים אוביר פרימיטיבי מודולו m . יהי $a \in \mathbb{Z}_m^*$. אז קיים $x \in \mathbb{Z}_m^*$ כך ש- $x^r \equiv a \pmod{m} \iff a^{\frac{\phi(m)}{\text{gcd}(\phi(m), r)}} \equiv 1 \pmod{m}$

טענה אם r, s זרים ל- $\phi(m)$ והופכיים $sr \equiv 1 \pmod{m}$ אז ההעתקה $f(x) = x^r \pmod{m}$ הנ"ל היא חח"ע ועל וההעתקה ההופכית לה היא $f(x) = x^s \pmod{m}$.

מקרה פרטי $r = 2$ נניח ש $m = p \geq 3$:

$$\frac{\phi(m)}{\gcd(\phi(m), 2)} = \frac{p-1}{2}$$

מסקנה אם p ראשוני אז קיים פיתרון ל- $x^2 \equiv a \pmod{p} \iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

הערה תמיד מתקיים $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$.

3.6 קונגרואציות ריבועיות

נדון בשאלה עובר אילו $a \in \mathbb{Z}_m^*$ קיים x כך ש- $x^2 \equiv a \pmod{m}$. אם יש משוואה דומה עם $a \notin \mathbb{Z}_m^*$ אז ניתן לצמצם אותה עד למצב הנ"ל.

טענה נניח $a \in \mathbb{Z}_m^*, m = m_1 m_2$ ו- $\gcd(m_1, m_2) = 1$ כאשר $m_1, m_2 > 1$. אז יש פיתרון ל- $x^2 \equiv a \pmod{m} \iff$ יש פיתרון ל- $x^2 \equiv a \pmod{m_1}, x^2 \equiv a \pmod{m_2}$.

מסקנה מספיק לדעת לפתור את המקרה $x^2 \equiv a \pmod{p^r}$.

3.6.1 סימן לגנדר

נניח $p \geq 3$ ראשוני ו- $a \in \mathbb{Z}_p$ נסמן

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \exists x. x^2 \equiv a \pmod{p} \\ -1 & \text{o.w.} \end{cases}$$

קריטריון אוילר

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}$$

מסקנה אם $p \geq 3$ ראשוני אז לכל $a, b \in \mathbb{Z}_m^*$ מתקיים

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \pmod{p}$$

שארית ריבועית נקרא ל- a שארית ריבועית מודולו m אם קיים x כך ש- $x^2 \equiv a \pmod{m}$.

טענה מספר השאריות הריבועיות מודולו p הוא $\frac{p-1}{2}$ כאשר $p \geq 3$ ראשוני.

מסקנה אם $p \geq 3$ ראשוני אז $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

משפט יהי $m = 2^k$.

כאשר $a \equiv 1 \pmod{m} \iff m$ שארית ריבועית מודולו $a, k = 1, 2, 3$
כאשר $a \equiv 1 \pmod{8} \iff m$ שארית ריבועית מודולו $a, k \geq 3$

משפט עבור ראשוני אי זוגי p ו- $a \in \mathbb{Z}_m^*$ אז a שארית ריבועית מודולו $p^r \iff a$ שארית ריבועית מודולו p .

משפט יהי $p \geq 3$ ראשוני. אז

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

3.6.2 הלמה של גאוס

יהי $p \geq 3$ ראשוני ו- $a \in \mathbb{Z}_m^*$. אז $\left(\frac{a}{p}\right) = (-1)^l$ כאשר

$$l = \left| \left\{ 1 \leq j \leq \frac{p-1}{2} \mid \text{the only representative of } j \cdot a \pmod{p} \text{ in the range } \left[-\frac{p-1}{2}, \frac{p-1}{2}\right] \text{ is negative} \right\} \right|$$

3.6.3 חוק ההדדיות הריבועית

נניח p, q ראשוניים.

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{1}{4}(p-1)(q-1)}$$

או באופן שקול:

$$\left(\frac{p}{q}\right) = (-1)^{\frac{1}{4}(p-1)(q-1)} \cdot \left(\frac{q}{p}\right)$$

3.6.4 סימן יעקובי

אם $m \in \mathbb{N}$ אי זוגי, נפרק אותו ל- $m = p_1 \cdot \dots \cdot p_k$ כאשר p_i ראשוניים אי זוגיים (מותר ריבוי).
אם $a \in \mathbb{Z}_m^*$ נגדיר את סימן יעקובי להיות

$$\left(\frac{a}{m}\right) = \prod_{i=1}^k \left(\frac{a}{p_i}\right)$$

אם $\gcd(a, m) > 1$ נסמן $\left(\frac{a}{m}\right) = 0$.
הערה - אם a שארית ריבועית מודולו m אז $\left(\frac{a}{m}\right) = 1$. בכיוון ההפוך זה לא תמיד נכון.

תכונות סימן יעקובי נניח n, m טבעיים אי זוגיים. אזי:

• אם a, b זרים ל- m אז

$$\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right) \left(\frac{b}{m}\right)$$

• אם a זר ל- m ול- n אז

$$\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right) \left(\frac{a}{n}\right)$$

•

$$\left(\frac{-1}{m}\right) = (-1)^{\frac{1}{2}(m-1)}$$

•

$$\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$$

•

$$\left(\frac{m}{n}\right) \left(\frac{n}{m}\right) = (-1)^{\frac{1}{4}(m-1)(n-1)}$$

4 קירובים דיפנטיים

משפט דיריכלה יהי $Q \geq 2$ טבעי ויהי $\theta \in \mathbb{R}$. אז יש מספר טבעי $1 \leq q < Q$ ושלים p כך ש-

$$|q\theta - p| \leq \frac{1}{Q}$$

או באופן שקול:

$$\left|\theta - \frac{p}{q}\right| \leq \frac{1}{qQ}$$

בפרט:

$$\left|\theta - \frac{p}{q}\right| \leq \frac{1}{q^2}$$

מסקנה אם $\theta \in \mathbb{R} \setminus \mathbb{Q}$, אז יש אינסוף רציונלים מצומצים $\frac{p_k}{q_k}$ שמקיימים:

$$\left|\theta - \frac{p_k}{q_k}\right| \leq \frac{1}{q_k^2}$$

4.1 שברים משולבים

כל רציונלי $\frac{p}{q}$ ניתן לרשום (לפי אלגוריתם אוקלידס) כשבר משולב:

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

כאשר $\forall i \geq 1, a_i \in \mathbb{N}, a_0 \in \mathbb{Z}$.

טענה אם $\forall i, a_i = b_i, m = n$ או שמתקיים $m \leq n, [a_0; a_1, a_2, \dots, a_n] = [b_0; b_1, b_2, \dots, b_m]$ או שמתקיים $n = m + 1, \forall 0 \leq i \leq m - 1, a_i = b_i, a_{m+1} = 1, a_m = b_m - 1$

מסקנה ההעתקה $cf : \{[a_0; a_1, \dots, a_n]\} \rightarrow \mathbb{Q}$ המעבירה שבר משולב לרציונלי היא על 2 ל-1

טענה נסמן $q_{-2} = p_{-1} = 1, q_{-1} = p_{-2} = 0$, בהינתן $[a_0; a_1, a_2, \dots, a_n]$ נגדיר נוסחאת נסיגה:

$$p_{k+1} = a_{k+1} \cdot p_k + p_{k-1}$$

$$q_{k+1} = a_{k+1} \cdot q_k + q_{k-1}$$

בכתיבה מטריצית:

$$\begin{bmatrix} p_{k+1} & p_k \\ q_{k+1} & q_k \end{bmatrix} = \begin{bmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{bmatrix} \begin{bmatrix} a_{k+1} & 1 \\ 1 & 0 \end{bmatrix}$$

אז

$$\frac{p_n}{q_n} = [a_0; a_1, a_2, \dots, a_n]$$

מסקנה לכל n

$$\det \begin{bmatrix} p_{k+1} & p_k \\ q_{k+1} & q_k \end{bmatrix} = \pm 1$$

וגם קיים $c > 0, \lambda > 1$ כך שלכל $n, q_n \geq c\lambda^n$

מסקנה נניח $a_0 \in \mathbb{Z}$ ולכל $i \in \mathbb{N}, a_i \in \mathbb{N}$ קיים הגבול

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

משפט לכל $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ יש סדרה a_0, a_1, \dots כך ש- $a_0 \in \mathbb{Z}$ ו- $a_1 \in \mathbb{N}$ $\forall i \geq 1$ המקיימת:

• אם $\frac{p_n}{q_n} = [a_0; a_1, a_2, \dots, a_n]$ אז לכל k :

$$\dots < \frac{p_{2k}}{q_{2k}} < \frac{p_{2k-2}}{q_{2k-2}} < \dots < \alpha < \dots < \frac{p_{2k+1}}{q_{2k+1}} < \frac{p_{2k-1}}{q_{2k-1}} < \dots$$

בפרט $\frac{p_k}{q_k} \rightarrow \infty$

• לכל n :

$$\frac{1}{a_{n+1} \cdot q_n^2} > \left| \alpha - \frac{p_k}{q_k} \right| > \frac{1}{(a_{n+1} + 2) \cdot q_n^2}$$

טענה יהי $\alpha \in \mathbb{Q}$. יש $C(\alpha) > 0$ כך שאם $\alpha \neq \frac{p}{q}$ אז $\left| \alpha - \frac{p}{q} \right| \geq \frac{C(\alpha)}{q}$.

מסקנה יש מספר סופי של קירובים "טובים" $\left| \alpha - \frac{p}{q} \right| < \frac{C(\alpha)}{q^2}$

משפט ההעתקה $cf : [a_0; a_1, a_2, \dots] \rightarrow \mathbb{R} \setminus \mathbb{Q}$ המוגדרת ע"י שברים משולבים היא חח"ע ועל.

4.2 מספרים אלגבריים וטרנסצנדנטיים

הגדרות מספר אלגברי הוא $\alpha \in \mathbb{C}$ שהוא שורש של פולינום עם מקדמים רציונליים. כך רציונלי הוא אלגברי. הדרגה של מספר אלגברי הוא ה- $d \geq 1$ המינימלי עבורו יש פולינום עם מקדמים רציונליים מדרגה d כך ש- α שורש שלו. דרגה של מספר רציונלי היא תמיד 1. מספר שאינו מספר אלגברי נקרא טרנסצנדנטי.

משפט ליוביל יהי α אלגברי מדרגה d .

אז יש $C(\alpha) < 0$ כך שלכל רציונלי $\alpha \neq \frac{p}{q}$ מתקיים $\left| \alpha - \frac{p}{q} \right| \geq \frac{C(\alpha)}{q^d}$

מקרה פרטי $d = 2$ מדיריכלה וליוביל:

$$\frac{C(\alpha)}{q^2} \geq \left| \alpha - \frac{p}{q} \right| \geq \frac{1}{q^2}$$

מסקנה נגדיר x להיות מקורב רע אם יש $C > 0$ כך שלכל p, q $\left| x - \frac{p}{q} \right| \geq \frac{C}{q^2}$. מסקנה אלגבריים מדרגה 2 הם מקורבים רע.

משפט קבוצת המספרים האלגבריים היא בת מנייה, והמרוכבים אינם.

משפט נסמן עבור $x \in \mathbb{R}$

$$\langle x \rangle = \min_{y \in \mathbb{Z}} |x - y| = \text{dist}(x, \mathbb{Z})$$

המכנים q_n של הקירובים $\frac{p_n}{q_n} = [a_0; a_1, \dots, a_n]$ עבור $\alpha = [a_0; a_1, \dots]$ מאופיינים ע"י התכונה הבאה:

$$\langle q_n \alpha \rangle = \min_{r \in \mathbb{R}} \langle r \alpha \rangle$$

יתרה מזאת:

• הסדרה $\langle q_n \alpha \rangle$ יורדת ל-0.

• לכל n ולכל $a, b \in \mathbb{Z}$, $1 \leq b < q_{n+1}$, מתקיים $|\langle b \alpha - a \rangle| \geq \langle q_n \alpha \rangle$

משפט לגרנז' x אלגברי מדרגה 2 $\iff x$ מחזורי ממקום מסוים

5 משוואת פל

נתון $D, D \in \mathbb{N}$ לא ריבוע.

ננסה למצוא את כל הפתרונות בשלמים הלא טריוויאליים למשוואה $\hat{}$

$$x^2 - Dy^2 = 1$$

(פיתרון טריוויאלי הוא $(x, y) = (\pm 1, 0)$)

טענה אם (x, y) פיתרון למשוואת פל, אז לכל n נרשום:

$$\bar{x}_n + \bar{y}_n \cdot \sqrt{D} (x + y \cdot \sqrt{D})^n (x - y \cdot \sqrt{D})^n$$

נקח $\bar{x}_n = x_n^2, \bar{y}_n = y_n^2$
אז כאשר x_n, y_n שלמים הם פתרונות למשוואת פל.

משפטים

- לכל D לא ריבוע יש למשוואת פל פיתרון לא טריוויאלי
- לכל D לא ריבוע כל הפתרונות הלא טריוויאליים מתקבלים מהטענה ומהחלפת סימונים.