

תורת הקוסינים

צורת: הרחבה של $\mathbb{Z}[\sqrt{-5}]$: $\mathbb{Z}[\sqrt{-5}] = \{x+y\sqrt{-5} \mid x,y \in \mathbb{Z}\}$

מונחים: חוק, חיסור, כפל.

פונקציית נורמה: $N(x+y\sqrt{-5}) = x^2+5y^2 = (x+y\sqrt{-5})(x-y\sqrt{-5})$: $N: \mathbb{Z}[\sqrt{-5}] \rightarrow \mathbb{Z}$

תכונות של נורמה:

$N(a) \geq 0$, $N(a) = 0 \Leftrightarrow a = 0$ *

$N(ab) = N(a) \cdot N(b)$ *

כזרה: $\alpha \in \mathbb{Z}[\sqrt{-5}]$ נהיה הפך אם קיים b . $ab=1$

נורמה: $1, -1$ הם היחידים שהפכים

הנחה: אם a הפך אזי $ab=1$ \Leftrightarrow $1 = N(1) = N(ab) = N(a) \cdot N(b)$

\Downarrow
 $N(a) = 1$
 $x^2 + 5y^2 = 1$
 $\Rightarrow y=0, x=\pm 1$

כזרה: מספר a הפך a יקרא א-פריק אם לכל פירוק $a=bc$ או b הפך

או c הפך (זהו פירוק טריוויאלי)

למשל 2 : $2 = (-2) \cdot (-1)$; 6 - פריק

צמצום מצד הנחה: $0 = 2 \cdot 3 = (1-\sqrt{-5})(1+\sqrt{-5})$ צמצום מצד הנחה

אי-פריקים!!

הנ"ל: הנספרים $1-\sqrt{-5}, 1+\sqrt{-5}, 2, 3$ הם א-פריקים ב- $\mathbb{Z}[\sqrt{-5}]$

הוכחה: נניח משערה $3=ab$ אזי $9 = N(3) = N(ab) = N(a)N(b)$

$N(a)=1, 3, 9$ \leftarrow	$N(a)=1$ אזי a הפך
$N(a)=9$ אזי b הפך	$N(a)=3$ אזי $N(a)=x^2+5y^2=3$
$N(a)=3$ אזי $N(a)=x^2+5y^2=3$	$x^2=3$ סתירה

\leftarrow 3 אי-פריק.

$4 = N(a) \cdot N(b)$

* נניח משערה $2=ab$ אזי

$N(a)=1, 2, 4$ \leftarrow	$N(a)=1$ אזי a הפך
$N(a)=4$ אזי b הפך	$N(a)=2$ אזי $N(a)=x^2+5y^2=2$
$N(a)=2$ אזי $N(a)=x^2+5y^2=2$	$x^2=2$ סתירה

סתירה \leftarrow הפך

$N(a) \cdot N(b) = 6$ אולי $(1+\sqrt{5})$ או $(1-\sqrt{5}) = ab$ (נ"ח) *

$N(a) = 1, 2, 3, 6 \leftarrow$ אולי $N(a) = 1, 6$ אולי a, b הפכים במחלקה
 $N(a) = 2, 3 \leftarrow$ אולי $N(a) = 2, 3$ - הרי חזי של אופשר בסדר מחלקה

! תקווה זה סקעי!

פירוק יחיד של שמים לאזורים ראשוניים:

הצבה: נני סקעי m מורכב אם אפשר זרמים אותו נרפסה $m=ab$, $a, b > 1$.

ראשוני = מספר סקעי לא מורכב, לכל 1 ו 0 .

יהי $a, b \geq 2$. a מורכב את b אם קיים $c \geq 2$ $a = bc$. (טובי ab)

תכונות של מורכב: (א) $a|a$, $a|0$

(ב) $a|b$, $b|a \iff a = \pm b$

(ג) $a|b$, $b|c \iff a|c$

(ד) $a|b$, $a|c \iff a|bx+cy \forall x, y \in \mathbb{Z}$

הצבה: אם a, b $a|a$ אמרם a מורכב שיש $b < a$.

! ראשוני - רק שני מחלקים חזיקים.

שאלות ותשובות על ראשוניים:

1. האם יש אינסוף? כן, אוקלידס הוכיח זאת. 2000 שנים.

2. בעיות מצדדך: האם נכון שיש מספר שלם מס' זוגי סקעי בדמ הוא סכום של שני ראשוניים - לא ידוע.

אם כן - מפתה: כן מס' אי זוגי זכור $n-7$ הוא סכום של שני ראשוניים.

הוכחה: $m = m + m$ אולי m זוגי, ומהפגרת מצדדך סכום של ראשוניים.

מסקנה זו נקראת בע"ת מצדדך (החנשה או האי צדית, אפשר להוכיחה כפי זה בתנן על הקוביות).

3. $\mathbb{R} < x < \infty$. $\left\{ \frac{1}{x} \mid x \text{ ראשוני} \right\} = \left\{ \frac{1}{p} \mid p < x \right\} = \mathcal{O}\left(\frac{1}{x}\right)$ עבור x זכור מפיסק. $\lim_{x \rightarrow \infty} \frac{\pi(x)}{x} = 1$

Prime Number Theorem A - על אזור

משפט: כן מס' שיש $N \neq 0 \in \mathbb{Z}$ הוא מרפסה של ראשוניים N זוגי -1 .

הוכחה: מפיסק עבור כל n .

כסס - 1 - מרפסה ראשוניים היתה
 -2 $\mathcal{O}\left(\frac{1}{x}\right)$ הורמו

נוכח שהורמו נמל קטנים $n-1$. אם n ראשוני n זוגי, אחרת n מרפסה שני.

מס' קטנים ממנו (אז n זוגי)

המשך תורת המספרים טיפוס 1.

כותמים $n = (\pm 1) p_1^{a_1} \dots p_k^{a_k}$, p_i מספרים ראשוניים, $a_i \geq 0$ מספרים טבעיים.

$$n = (-1)^{\sum \alpha(p)} \prod_{p \in P} p^{\alpha(p)} \rightarrow \alpha(p) \in \mathbb{Z}, \alpha(p) \geq 0: \alpha(p) = \sum \alpha_i p_i$$

מתקיים: $\alpha(p) \geq 0$ מספר החזקות של p במספר n .
 P - קבוצת המספרים הראשוניים.
 $\sum \alpha(p) = \Omega(n)$ - מספר המספרים הראשוניים המופיעים בפרק.

הצבה: יהי $\mathbb{Z} \neq n + 0$ או $\mathbb{Z} \neq a$, $a \in \mathbb{Z}$, a גדול מ-0 או $a < 0$ ו- $n \neq 0$.

אבל $n \nmid a$. אומרים ש- a חסר חלקים מש- n . $a = ord_p(a)$

משפט: לכל $a \in \mathbb{Z}$, $a \neq 0$ קיים פירוק $n = (-1)^{\sum \alpha(p)} \prod_{p \in P} p^{\alpha(p)}$

הוכחה: $\{$ היותו של a חסר חלקים מש- n שיהיה שיהיה a חסר חלקים מש- n .
 $\} \rightarrow$ (הפונ' נקבעת בהיחזור)

משפט: חתום עם שארית. $a, b \in \mathbb{Z}$, $a \neq 0$ אזי קיימים $r, q \in \mathbb{Z}$ ו- $0 \leq r < |a|$.

$$a = bq + r, \quad 0 \leq r < |a|$$

הוכחה: נסתכל על הקבוצה של מספרים $a - bx$, $x \in \mathbb{Z}$. קבוצה

מכילה מספרים חיוביים. יהי r המינימום של המספרים החיוביים ביותר בקבוצה.

אנו טוענים $0 \leq r < |a|$. אם $a > 0$ אז $r = a - bx$ ו- $0 \leq r < a$ (הוא חיובי).

$$r = a - bx, \quad q = x$$