

מספרים ראשוניים

סימון - n מספר, כשנבין n , נת"חם n ראשוניים החלובים

מסקנה - $n \in \mathbb{N}$, $n > 1$, יש n ראשוניים p_1, \dots, p_k ראשוניים טונים
 $n = p_1^{r_1} \cdot \dots \cdot p_k^{r_k}$
 ג'יבוק זה יחיד עד כדי שינוי סדר.

הערה - קשה לתת פירוק פורמלי ראשוניים של מספר גדול
 ק' למצוא מתק מנותן מקסימל' של 2 מספרים גדולים (באמצעות אלגוריתם אוקלידס)

מספר אוקלידס - יט אוינסל ראשוניים

הערה - קשה מאוד לרשום באופן מפורט ראשוניים גדולים

הפונקציה $\pi(x)$ - (מס' את הראשוניים בסדר עולה $p_1 < p_2 < \dots < p_k < \dots$, $p_1=2, p_2=3, p_3=5, \dots$)

$\pi(x) = \#\{k \mid p_k \leq x\}$ - 51

שאלה חשובה - גאינה קצב ג'ילה הפונקציה $\pi(x)$?

מספר המספרים הראשוניים!
 $\pi(x) \sim \frac{x}{\log x}$

(סימון \sim - הפע גדלות באותו קצב)

כאמר - אם יש n מספרים n - x , כ- $\frac{1}{n}$ מהמספרים הקטנים n - x הם ראשוניים.

לא נכוח את זה בקורס.

משפט - משפט זנון
 קיימים קבועים c_1, c_2 חיוביים ו- ψ כגון $c_1 \frac{x}{\log x} \leq \pi(x) \leq c_2 \frac{x}{\log x}$

נוכח בהמשך.

$p_1 \leq 2^{2^l}$, $l \in \mathbb{N}$ - עכס

$\pi(x) \geq \log(\log(x))$, עכס $x \geq 2$ - מסקנה

$q_l = p_1 \dots p_{l+1}$, $p_{l+1} \leq q_l$ - הוכחת המשנה (נסמן)

$2^{2^l} = 4 \Rightarrow p_1 = 2$, נוכח האינדוקציה. עבור $l=1$

$p_{n+1} \leq q_n = p_1 \dots p_n + 1 \leq 2^{2^1} \cdot 2^{2^2} \dots 2^{2^n} + 1 = 2^{2^1+2^2+\dots+2^n} + 1 = 2^{2^{n+1}-2} + 1 \leq 2^{2^{n+1}}$

הוכחת המשנה - נניח תחילה $x > e^{e^3}$

$e^{e^{n-1}} < x \leq e^{e^n}$ - קיים n טבעי כך ש-

$\pi(x) \geq \pi(e^{e^{n-1}}) \geq \pi(2^{2^n}) \geq \pi(p_n) = n = \log \log(e^{e^n}) \geq \log \log(x)$

אם $5 \leq x \leq e^3$: $\log \log(x) \leq 3$

$\pi(x) \geq \pi(5) = 3 \geq \log \log(x)$

אם $2 \leq x \leq 5$ - תרצה

הוכחה של ארטוסטנס

כדי למצוא את הראשונים עד N , הוסיף את $1, \dots, N$, מסומן את כל הפריקים של 2 . מסומן את המספר הראשון שלא סומן. קוראים לו p_2 , ומחזקים את כל הפריקים שלא מסומנים.

מספרי פרמה

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

כמה נחם שכל F_n ראשוני. מצעכייט הוא טעה.

מספרי מרסן

$M_n = 2^{p_n} - 1$

p_n - ראשוני.

מרסן חתק שהוא יוקצ את כל ה M_n הראשוניים עד $p_n \leq 200$. אם הוא קצת טעה.

המאה ה-19 קדם הוכחה ראשוני מוצא ביטוי הנחה את כל הראשוניים הקטנים $10^6 \cdot 100$. זה לקח 20 שנה, 8 כרכים, 420 עמודים, ואחד הקבלים אבד.

בצורת מחשבים, אפשר לחשוב את כל המשוואות של הקורס יום ביומם 37.6 לשלם

אנחנו נבין במציאת המשוואות גדולות בהרבה (אך לא נכלל לעבוד את כלם)

מספרים פרימים גדולים
 * הפרטים נוספות על מספרים פרימים: $F_n = 2^{2^n} + 1$
 פרימה ראשונה - F_0, F_1, F_2, F_3, F_4 המשוואות ושיעור שכלים
 אוליגרה הוכיחה ש- F_5 פריק, ומאידך הצליחו לסדר את $F_6, F_7, F_8, F_9, F_{10}$ וכו' (אמנם לא)

טענה - לכל m, n , $\gcd(F_n, F_m) = 1$

מסקנה - יש אינסוף ראשוניים (כי לאף אחד מהם F_n אין מחלקים ראשוניים)

הוכחת הטענה:
 נעזר בצורת:

$$(n \text{ אינטי}) \quad x^n - x^{n-1} + x^{n-2} + \dots + x - 1 = \frac{x^n - 1}{x + 1}$$

נניח $n = 2^m$, נבחר $x = 2^{2^k}$, $m = n + k$

$$F_m = 2^{2^m} + 1 = 2^{2^n \cdot 2^k} + 1 = (2^{2^n})^{2^k} + 1 = x^{2^k} + 1$$

$$\frac{F_m - 2}{F_n} = \frac{x^{2^k} - 1}{x + 1} = x^{2^k-1} + x^{2^k-2} + \dots - 1 \in \mathbb{N} \rightarrow F_n | F_m - 2$$

$d = \gcd(F_n, F_m)$ מחלק את F_n , $F_m - 2$, ולכן את F_m , אך $d \nmid 2$
 $d = 1$ כי F_n אינטי

מספרי מרסן - הטענה

$$M_p = 2^p - 1 \quad \text{כאשר } p \text{ ראשוני}$$

מרסן טען ש- M_p ראשוני עבור $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$
 בהשערה הן כמה טעויות

ב- 1903 הקיפה קדם בהתבטאה של שפה בארה"ב ש- $2^{67} - 1$ אינטי פריק, ע"י הכפלת שני מספרים שלק"ם.

שאלה פתוחה: האם יש אינסוף מספרי מרסן ראשוניים? או פריקים?

* המספר הראשוני הגדול ביותר הידוע היום הוא M_p כאשר $p = 74, 207, 281$
 יש בו כ-10.2 ספרות בקב"ס 10, או ספר בן 6000 ספרות.

משפט צ'ביטב

תוצאות - ישם קבועים חיוביים C_1, C_2 מתקיים: $(x^2) \quad C_1 \frac{x}{\ln x} \leq \pi(x) \leq C_2 \frac{x}{\ln x}$

* במסל של הפונקציה $\frac{x}{\ln x} = \int_1^x \frac{1}{\ln t} dt$ ובהתקדם נגזרת חיובית עבור $x > e$, צי שהוכיח את המשפט עבור $x > e$ - x כלשהו (כי ברור שהיא חסומה בקטע סגור ממשי ואינטי).

מסקנות - א - קיים קבועים חיוביים α, β כך שכל K :
 $\alpha K(\log K) \leq P_K \leq \beta K(\log K)$

ב - $\sum_{k=1}^{\infty} \frac{1}{k^2}$ מתכנס

$$\sum_{k=1}^{\infty} \frac{1}{k^2} \geq \beta \sum_{k=1}^{\infty} \frac{1}{K(\log K)}$$

נוכיח את א' < ב' :

$$\int_1^{\infty} \frac{1}{x \ln x} dx = \lim_{T \rightarrow \infty} \log(\log x) \Big|_{x=1}^{x=T} = \log \log T - \log \log 1$$