

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

נוכח בהמשך.

לענה - לכל $l \in \mathbb{N}$, $p_l \leq 2^{2^l}$

הסקנה - לכל $x \geq 2$, $\pi(x) \geq \log(\log(x))$

הוכחת הלענה - (נסח)
 $q_l = p_1 \cdot \dots \cdot p_l + 1$, $p_{l+1} \leq q_l$

$$2^{2^1} = 4 \geq p_1 = 2$$

נוכח באינדוקציה. עבור $l=1$,

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

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

קיים n טבעי כך ש-

$$e^{e^{n-1}} < x \leq e^{e^n}$$

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

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 ארסטוסטס

כדי למצוא את הראשוניים עד N , הופספים את $1, \dots, N$, מסמלים את כל הפסוקים של 2. מסמלים את המספר הראשוני שלא סומן. קוראים לו p_2 , ואחרים את כל הפסוקים שלא מסמלים.

מספרי פרמה

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

פרמה ניחש שכל F_n ראשוניים. הצעתי הוא טעה.

מספרי מילר

$$M_n = 2^{p_n} - 1$$

p_n - ראשוני.

מילר חשק שהוא יוכיח את כל ה- M_n הראשוניים עד $p_n \leq 200$. אם הוא קצת טעה.

המאה ה-19 קדם האסטרי מוצא בשיטה הנכונה את כל הראשוניים הקטנים מ- 10^6 . 100. זה לקח 20 שנה, 8 כרכים, 4202 עמודים, ואחד הערכים אבד.

בצורת מחשבים, אפשר לחשב את כל המספרים עד 10^9 בשני דקות.

אנחנו נבין במציאת האטונים גדולים בהרבה (אך לא נוסף למצוא את כלם).

מספר פרמה: $F_n = 2^{2^n} + 1$.
 פרמה ראה ש- F_0, F_1, F_2, F_3, F_4 הם ראשוניים ושיש שברור ש- F_n לא מתחלק ב- F_m עבור $n < m$.
 שכל המספרים פרמית.

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

מסקנה - יש אינסוף ראשוניים (כי לכל F_n מתחלק מה- F_n אין מחלקים ראשוניים).

הוכחת הטענה:
 נעזר בצורות:

$$(x^n - 1) = (x - 1)(x^{n-1} + x^{n-2} + \dots + x + 1)$$

נניח $m = n + k$, $x = 2^{2^n}$, $F_n = x + 1$

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

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

$d = \gcd(F_n, F_m)$
 $d | F_n$ ו- $d | F_m - 1$, ולכן $d | 1$, כלומר $d = 1$.

מספר מרסן - הערה

$$M_p = 2^p - 1$$

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

ב-1903 הקיבוץ קדם בהצגה של שעה בארבע ש- $2^{67} - 1$ היה פרק, ע"י הכפלת שני מספרים שלק"ם.

שאל פתוחה: האם יש אינסוף מספר מרסן ראשוניים? או פריקים?

המספר הראשוני הגדול ביותר הידוע היום הוא M_p כאשר $p = 74,207,281$.
 יש בו כ-10 מיליארד ספרות בבסיס 10, או סביב 6000 סיביות.

משפט צ'ביצ'ב

$$C_1 \frac{x}{\log x} \leq \pi(x) \leq C_2 \frac{x}{\log x} \quad (x \geq 2) \quad C_1, C_2 \text{ חיוביים}$$

המשפט של דהפונקציה $\pi(x) = \frac{x}{\log x}$ נכונה, והפונקציה $\pi(x)$ חלוקת צ'ביצ'ב, צי שהוכיח את המשפט.
 צ'ביצ'ב הראה ש- $\pi(x) \sim \frac{x}{\log x}$ (כי ברור שהיא חסומה בקטע סגור, ממעט ווייטס וטאסיהצ'ב).

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

$$\sum_{k=1}^{\infty} \frac{1}{k^2} \geq \frac{1}{2}$$

נוכיח את א' < ב' :

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