

הגדרה 1:

יהיו a, b מספרים שלמים. אומרים כי b מחלק את a אם קיים מספר שלם q כך ש-

$$a = qb.$$

כלומר $\frac{a}{b}$ שווה למספר שלם q .

הסימון $b \mid a$ אומר כי b מחלק את a .

משפט 1: קיימים אינסוף מספרים ראשוניים

קיימים אינסוף מספרים ראשוניים.

הוכחה: נוכיח הטענה דרך השלילה.

נניח כי $\{p_1, \dots, p_n\}$ הוא הקבוצה של כל הראשוניים שקיימים וקבוצה זו נוצרת סופי.

נגדיר השלם $M = (p_1 \cdot p_2 \cdot \dots \cdot p_n) + 1$.

לפי משפט הפירוק לראשוניים (ראו משפט ?? למעלה או משפט ?? למטה) M הוא מספר ראשוני או שווה למכפלה של ראשוניים.

M לא מספר ראשוני בגלל ש- $M > p_i$ לכל $1 \leq i \leq n$.

גם לא קיים מספק ראשוני p_i אשר מחלק את M . הרי

$$M \% p_i = 1 \Rightarrow p_i \nmid M.$$

הגענו לסתירה של המשפט הפירוק לראשוניים, לכן קיימים אינסוף מספרים ראשוניים. ■