<u>הוכחת המשפט הקטן של פרמה:</u>

נתון מספר ראשוני p.

יהי a מספר שלם חיובי אשר p אינו מחלק שלו (למעשה זו דרישה חלשה יותר מ- $1 \le a \le p-1$).

נרשום את $p-1$ הכפולות הבאות של a:

$$a, 2a, 3a, \dots, (p-1)a$$

ברור כי p אינו מחלק של אף אחת מהכפולות הנ"ל.

נסתכל כעת על קבוצת הערכים שמתקבלת ע"י ביצוע $(\text{mod } p)$ לכל אחד מהערכים הנ"ל. כלומר על הקבוצה:

$$B = \{\, a\ (mod\ p), 2a(mod\ p), 3a(mod\ p), \dots, (k-1)a(mod\ p)\,\}$$

ראשית נראה כי בקבוצה B כל האיברים שונים זה מזה.

נניח בשלילה שקיימים שני ערכים $ra, sa \in B$ כך ש $1 \le s < r \le p-1$ ומתקיים ש:

$$ra \equiv sa\ (mod\ p)$$

מכיוון ש p אינו מחלק של a ניתן להסיק ש:

$$r \equiv s(mod\ p)$$

וזה לא ייתכן כי אז p מחלק את $r-s$, בסתירה לכך ש $1 \le (r-s) < p-1$ ו- p ראשוני.

לכן, B מכילה $p-1$ ערכים שונים זה מזה בין 1 ל $(p-1)$ כולל . כלומר תכיל את קבוצת הערכים $1,2,\dots,p-1$ בסדר כלשהו.

אם נסתכל על מכפלת הערכים בקבוצה B יתקיים ש:

$$a \cdot 2a \cdot 3a \dots \cdot (p-1)a \ \equiv 1 \cdot 2 \cdot \dots \cdot (p-1)\ (mod\ p)$$

כלומר:

$$(p-1)! \cdot a^{p-1} \equiv (p-1)!\ (mod\ p)$$

מכיוון ש p ראשוני הוא אינו מחלק של $(p-1)!$ ולכן מתקיים:

$$a^{p-1} \equiv 1\ (mod\ p)$$

ההוכחה לקוחה מ: https://primes.utm.edu/notes/proofs/FermatsLittleTheorem.html