מספרים ראשוניים:

המשפט היסודי של האריתמטיקה - פירוק לראשוניים

לכל מספר קיים פירוק יחיד לראשוניים. כלומר: קיימים כך ש: .

הוכחה: **קיום** - נוכיח באינדוקציה חזקה על :   
בסיס: - הוא ראשוני וזהו גם הפירוק.

צעד: נניח שלכל מספר עד קיים פירוק לראשוניים ונוכיח שגם ל קיים פירוק.  
נחלק למקרים: אם ראשוני אז הוא הפירוק של עצמו.  
אחרת, פריק ולכן קיימים שלמים חיוביים כך ש:   
לפי הנחת האינדוקציה, קיים פירוק ל וקיים פירוק ל   
כלומר: , כאשר: ראשוניים.  
.

מכאן, הפירוק של n הוא:   
(אם יש ראשוניים שחוזרים על עצמם ניתן לחברם ע"י חוקי חזקות)

**יחידות** - נניח בשלילה שקיימים 2 פירוקים שונים כך ש: כאשר

ראשוניים לאו דווקא שונים. מכאן:   
טענת עזר (הלמה של אוכלידס): אם כאשר p ראשוני, אזי קיים כך ש .

לפי טענת העזר נובע שקיים כך ש: . ראשוני ולכן: (כי גם ראשוני)  
כעת, נחלק את 2 צדדי השוויון ב . נחזור על התהליך שוב ושוב באותו האופן. מכאן: אם נקבל בסופו של דבר בצד אחד מכפלת ראשוניים ובצד השני - 1. סתירה כי לא ייתכן שמכפלת ראשוניים (או אפילו ראשוני אחד) תהיה שווה 1.  
אם אז נקבל שכל הראשוניים בצד שמאל שווים בדיוק (גם בכמות) לכל הראשוניים בצד ימין - סתירה לכך שאלו פירוקים שונים.

תרגיל: הוכיחו שלכל מספר פריק, קיים ראשוני כך ש .

הוכחה: מכיוון ש פריק, קיימים שלמים כך ש: . בהכרח לפחות אחד מבין קטן או שווה ל . (כי אחרת, אם אז: וזו סתירה.) בה"כ (בלי הגבלת הכלליות) נאמר ש . לפי המשפט היסודי של האריתמטיקה, קיים פירוק ל לראשוניים, בפרט יש ראשוני כך ש . מכאן: וגם: .

קיום אינסוף ראשוניים:

ההוכחה של אוקלידס: נניח בשלילה שקיימים רק מספר סופי של ראשוניים: (כלומר, יש רק k ראשוניים כאשר k מספר שלם חיובי). נגדיר: . לפי המשפט היסודי של האריתמטיקה, ל יש פירוק לראשוניים. לכן קיים כך ש . אבל ולכן: אבל ראשוני ולא יכול להיות 1 - סתירה.

הוכיחו: קיימים אינסוף ראשוניים מהצורה:   
מבין שאריות החלוקה ב 6: רק יכולים לייצג מספרים ראשוניים.  
נניח בשלילה שקיימים רק מספר סופי של ראשוניים מהצורה הנ"ל: (כלומר, יש רק k ראשוניים כאשר k מספר שלם חיובי). נגדיר: . לפי המשפט היסודי של האריתמטיקה, ל יש פירוק לראשוניים. לא ייתכן שהוא בקבוצה S כי אחרת אם קיים כך ש אז ולכן: אבל ראשוני ולא יכול להיות 1 - סתירה.  
בנוסף, לא ייתכן שכל הראשוניים של מהצורה כי אחרת גם הוא היה מהצורה הזאת (כי המכפלה: שומרת על הצורה)  
ולכן לפחות ראשוני אחד חייב להיות מהצורה: וכפי שראינו, הוא לא ב S - סתירה לכך שיש רק k ראשוניים מהצורה הנ"ל.