הוכחה למשפט היסודי של האריתמטיקה
מאת: עריסטו

המשפט היסודי של האריתמטיקה: כל מספר טבעי ניתן לבטא בדרך אחת בדיוק כמכפלה של מספרים ראשוניים.
נוכיח את המשפט.
ראשית, לכל מספר טבעי יש לפחות פירוק אחד לגורמים ראשוניים, שכן אם המספר פריק ניתן לפרקו לשני גורמים שלמים גדולים מ – 1, לפרק כל אחד משני הגורמים האלה (אם הוא פריק) לשני גורמים כנ"ל וכן הלאה; התהליך הזה חייב להסתיים כי הגורמים של כל מספר קטנים ממנו, וכאשר הוא מסתיים – מצאנו פירוק של המספר המקורי לגורמים ראשוניים.
אם קיים מספר שהוא בעל שני פירוקים שונים לגורמים ראשוניים, נקרא למספר הקטן ביותר בעל תכונה זו N. כאשר $N = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$, p ו- q ראשוניים. אנו יכולים להניח ש- $p_1 \le p_2 \le \ldots \le p_n$ ו- $q_1 \le q_2 \le \ldots \le q_m$. שימו לב לכך ש- $p_1 \ne q_1$, אחרת $\frac{N}{p_1} = \frac{N}{q_1}$ הקטן מ- N היה בעל שני פירוקים שונים, בניגוד להנחה. נניח ש- $p_1 < q_1$.

$N' = p_1(p_2 p_3 \cdots p_n - q_2 q_3 \cdots q_m) = (q_1 - p_1) q_2 q_3 \cdots q_m$ הוא חיובי וקטן מ- N. לכן, לפי הנחתנו, ל- N' יש פירוק יחיד לגורמים ראשוניים. p_1 הוא גורם של N' ולכן הוא מתלכד עם אחד הגורמים q_2, q_3, ..., q_m או מחלק את $q_1 - p_1$. אי-השוויונים $p_1 < q_1 \le q_2 \le \ldots \le q_m$ מראים שהמקרה הראשון הוא בלתי אפשרי. לכן, p_1 מחלק את $q_1 - p_1$. אבל במקרה זה p_1 מחלק את q_1 - דבר הסותר את העובדה ש- q_1 הוא ראשוני. לכן, הנחתנו אינה נכונה, דבר המשלים את הוכחת המשפט.