©צוות קורס "תורת המספרים האלגוריתמית" סמסטר א תש"פ: בר אלון, מיכאל פרי, שמואל שמעוני, איברהים שאהין, דורון מור, חיה קלר, אלעד אייגנר-חורב. נכתב ע"י דורון מור

פירוק ייחודי לגורמים ראשוניים

הגדרה: מספר טבעי חיובי ייקרא **ראשוני** אם זה גדול מ-1 ומתחלק אך ורק בעצמו וב-1.

דוגמות: $2,3,5,7,11$ הם המספרים הראשוניים הקטנים ביותר. אפשר למצוא גם את $41, 43, 47, 53, 59, 61$ כמספרים ראשוניים יותר גדולים, ואת $7211, 7213$. כמה ראשוניים יש בעולם?

הגדרה: מספרים טבעיים שאינם ראשוניים נקראים **פריקים**. כלומר, n פריק אם קיימים $2 \le a, b < n$ כך ש $n = ab$.

דוגמות: $30 = 2 \cdot 3 \cdot 5$ ולכן הוא פריק, וכן גם $42 = 2 \cdot 3 \cdot 7$. גם המספר $999 = 3 \cdot 3 \cdot 3 \cdot 37$ פריק.

הגדרה: הראשוניים השונים המופיעים בפירוק של מספר נקראים ***גורמים ראשוניים*** של המספר.

הגדרה: נאמר כי b מחלק את a ונסמן $b|a$ אם קיים k שלם כך ש $kb = a$.

למה 1: יהיו a, b, n מספרים טבעיים. אם $a|n$ וגם $b|a$ אזי $b|n$.

הוכחה: לפי ההנחה $n = aq$ וגם $a = bk$ עבור q, k שלמים כלשהם. לכן מתקיים

$n = aq = bkq$ ולכן הטענה מתקיימת. ■

למה 2: לכל מספר שלם גדול מ-1 יש מחלק ראשוני.

הוכחה: נניח בשלילה שהטענה איננה נכונה, ויהי n דוגמה נגדית מינימלית לטענה (קיומה מובטח כעת לפי ההנחה בשלילה ולפי WOP). ניתן לקחת n שאינו ראשוני, שכן אחרת אינו מהווה דוגמה נגדית. לכן n פריק, וניתן לרשום $n = ab$ עבור $2 \le a, b < n$ כלשהם. היות ו-n הוא דוגמה נגדית מינימלית, a אינו מפר את הלמה (שכן $a < n$). ולכן ל a יש מחלק ראשוני. נובע שגם ל-n יש מחלק ראשוני לפי למה 1. סתירה. ■

משפט 3: אם n פריק, אזי יש לו מחלק ראשוני שאינו גדול מ $\sqrt{n}$.

הוכחה: נרשום $n = ab$, כאשר $2 \le a, b < n$. אנו רשאים להניח כי $a \le \sqrt{n}$ שכן אם $a, b > \sqrt{n}$ אזי $ab > n$. לפי למה 1, ל-a יש מחלק ראשוני, שבפרט מחלק את n לפי למה 2. ■

משפט 4 (המשפט היסודי של האריתמטיקה): כל מספר שלם גדול מ-1 יכול להירשם בצורה יחידה

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$$

כאשר לכל $i \in [k]$ מתקיים $a_i > 0$, כל p_i הוא ראשוני וגם $p_1 < p_2 < \cdots < p_k$.

הוכחה ראשונה: נפצל את ההוכחה לשני חלקים: תחילה נוכיח קיום של הפירוק, כלומר, שיש לפחות דרך אחת לכתוב את המספר כמכפלה של ראשוניים. שנית, נוכיח יחידות של הפירוק. כלומר, שאם יש כמה פירוקים אפשריים לראשוניים, אזי הם זהים עד כדי סדר הראשוניים במכפלה.

קיום: נניח בשלילה כי הטענה שלילית וקיימים מספרים טבעיים חיוביים שלא יכולים להירשם כמכפלת ראשוניים. יהי n דוגמה נגדית מינימלית. ננתח את הדוגמה הזו. המספר n אינו ראשוני, אחרת אינו מהווה דוגמה נגדית. לכן, n פריק, וניתן לרשום $n = ab$ עבור שני מספרים $2 \le a, b <$

n. היות ו-n דוגמה נגדית מינימלית, המספרים a,b אינם דוגמה נגדית, ולכן ניתן לרשום אותם כמכפלת ראשוניים. לכן, גם את n ניתן לרשום כמכפלת ראשוניים. סתירה.

<u>יחידות</u>: נניח שקיים מספר n עבורו קיימים שתי מכפלות ראשוניים שונות. כלומר

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots \cdot q_s$$

נבחר את n כך שבין שני הייצוגים הללו אין אף ראשוני משותף (לחלופין, נחלק את הייצוגים בכל הראשוניים המשותפים כך שנישאר ללא ראשוניים זהים). היות ומתקיים $p_1(p_2 \ldots p_k) = q_1 q_2 \ldots q_s$ נקבל ש $p_1 | q_1 q_2 \ldots q_s$, ולכן קיים $i \in [s]$ כך ש $p_1 = q_i$. סתירה. ■

בעבר הזכרנו ש-*WOP* שקול לאינדוקציה. לכן, נראה עכשיו הוכחה באינדוקציה למשפט היסודי של האריתמטיקה.

<u>הוכחה שנייה</u>:

<u>קיום</u>: ההוכחה באינדוקציה על n. הטענה נכונה עבור $n = 2$. נניח שהיא נכונה עבור כל המספרים עד n. אם n ראשוני- סיימנו. לכן, נניח ש-n פריק, כלומר, $n = ab$ עבור $2 \leq a,b < n$. לפי הנחת האינדוקציה, a וגם b הם ראשוניים או שניתן לבטא אותם כמכפלת ראשוניים, ולכן גם את n.

<u>יחידות</u>: ההוכחה באינדוקציה על n. הטענה נכונה עבור $n = 2$. נניח שהטענה נכונה לכל המספרים $1 < k < n$. נניח גם כי n פריק ויכול להירשם כמכפלת ראשוניים (הוכחנו את זה ב<u>קיום</u>). נשאר להראות את היחידות של הפירוק לראשוניים. נניח בשלילה כי קיימים שני פירוקים אפשריים, כלומר,

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots \cdot q_s$$

נראה ש $k = s$, וששני הפיקטורים מכילים את אותם הראשוניים, באותה כמות של פעמים. היות ומתקיים $p_1(p_2 \ldots p_k) = q_1 q_2 \ldots q_s$, נקבל ש $p_1 | q_1 q_2 \ldots q_s$, ולכן קיים $i \in [s]$ כך ש $p_1 = q_i$. בלי הגבלת הכלליות (בה"כ מכאן והלאה) נניח ש $i = 1$. היות ו-n פריק, בהכרח $k > 1, s > 1$, ולכן $1 < n/p_1$. הנחת האינדוקציה עבור n/p_1 מבטיחה שלמספר זה יש פיקטור יחיד, ולכן $k = s$ והפיקטור של n יחיד. ■