21/11 בס"ד

המשפט היסודי של האריתמטיקה

א) מספרים ראשוניים ופריקים

מספר ראשוני- הוא מספר שלם וחיובי הגדול מ-1, ומתחלק אך ורק בעצמו וב-1.
נסמן בדרך כלל ב-p (Prime number).

מספר פריק- כל מספר שלם וחיובי שאינו ראשוני ואינו 1 יקרא פריק. כלומר שאם n מספר פריק אז קיימים $a,b\in\mathbb{N}$ כך ש-$2\le a,b<n$, ומתקיים: $a\cdot b=n$.

מחלק ראשוני- הם המספרים הראשוניים המופיעים בפירוק של מספר. לדוגמא: בפירוק של $12=3\cdot4$
3 הוא המחלק הראשוני של 12.

ב) מחלק ראשוני

(1) משפט: לכל מספר שלם הגדול מ-1 יש מחלק ראשוני.

הוכחה: נניח בשלילה שהטענה אינה נכונה, וכי קיימת קבוצה של מספרים שלמים הגדולים מ-1 שאין להם מחלק ראשוני. לפי ההנחה הקבוצה אינה ריקה, ולכן לפי עקרון ה-W.O.P קיים איבר מינימלי בקבוצה זו שנקרא לו n. n איננו מספר ראשוני שכן אחרת הוא המחלק הראשוני של עצמו, ולכן הוא פריק. מכיוון ש-n פריק קיימים $a,b\in\mathbb{Z}$ כך ש-$2\le a,b<n$ המקיימים $n=a\cdot b$. היות ו-$a<n$, ו-n הוא האיבר המינימלי שאין לו מחלק ראשוני, אזי ל-a כן יש מחלק ראשוני, כלומר שקיים p ראשוני ו-$k\in\mathbb{Z}$ כך ש-$p\cdot k=a$. נמצא אם כן שמתקיים: $n=p\cdot k\cdot b$, כלומר ש-$p|n$ וזוהי סתירה. נמצא אם כן שלכל מספר שלם הגדול מ-1 יש מחלק ראש

(2) משפט: לכל מספר n שלם ופריק הגדול מ-1 יש מחלק ראשוני שאינו גדול מ-$\sqrt{n}$, כלומר,
אם $p|n$ אזי $p\le\sqrt{n}$.

הוכחה: מכיוון ש-n פריק קיימים $a,b\in\mathbb{Z}$ כך ש-$2\le a,b<n$ המקיימים $n=a\cdot b$. ניתן להניח כי לפחות אחד מ-a או b קטן או שווה ל-$\sqrt{n}$, שכן אחרת $n<a\cdot b$, נניח שזהו a. לפי משפט קודם האומר שלכל מספר שלם הגדול מ-1 יש מחלק ראשוני, אזי ל-a יש מחלק ראשוני $p\le a\le\sqrt{n}$ המקיים $p|a$, ולכן קיים $k\in\mathbb{Z}$ כך ש-$p\cdot k=a$. נמצא ש-$n=p\cdot k\cdot b$ ולכן p הוא מחלק ראשוני של n, המוכיח את המשפט.

(3) משפט: יהיו $a,b\in\mathbb{Z}$ ויהי p מספר ראשוני. אם $p|ab$ אזי $p|a$ או $p|b$.

הוכחה: נניח בשלילה כי $p\nmid a,b$. אזי בגלל הגדרת מספר ראשוני מתקיים $(p,a)=1$. אזי לפי משפט (2) ב-gcd $p|b$ שזו סתירה. לכן p מחלק לפחות את a או את b.

21/11

בס"ד

ג) המשפט היסודי של האריתמטיקה

משפט:

כל מספר שלם וגדול מאחד $1<n$, ניתן להציג אותו באופן יחודי כמכפלה של ראשוניים בלבד מהצורה הבאה: $n = p_1^{a_1}\cdot p_2^{a_2}\cdot p_3^{a_3}\cdot\ldots\cdot p_k^{a_k}$

כאשר לכל $i\in[k]$ מתקיים: (1) p_i מחלק ראשוני של n כך ש-$p_1<p_2<\ldots<p_k$

(2) $a_i\geq 1$.

הביטוי $p_1^{a_1}\cdot p_2^{a_2}\cdot\ldots\cdot p_k^{a_k}$ נקרא "הפקטוריזציה של n למחלקיו הראשוניים".

נמצא אם כן שמספרים ראשוניים הם כמו אטומים שניתן להרכיב מהם כל מספר אך אותם לא ניתן לחלק.

דוגמאות:

$240 = 2\cdot 2\cdot 2\cdot 2\cdot 3\cdot 5 = 2^4\cdot 3\cdot 5 \qquad 2<3<5$

$1001 = 7\cdot 11\cdot 13 \qquad 7<11<13$

משפט עזר:

לפני שנוכיח את המשפט היסודי נוכיח משפט נוסף שיעזור לנו בדרך ההוכחה של המשפט היסודי.

משפט: יהי p מספר ראשוני ויהי $q_1,q_2,\ldots,q_n\in Z$. אם מתקיים $p|q_1\cdot q_2\cdot\ldots\cdot q_n$ אזי קיים $j\in[n]$ כך ש-$p|q_j$.

הוכחה: באינדוקציה על n.

בסיס- עבור $n=1$ הטענה טריוויאלית כי אכן $p|q_n=q_j$. גם עבור $n=2$ הוכחנו בסעיף קודם

צעד- נניח כי אם $p|q_1\cdot q_2\cdot\ldots\cdot q_n$ אזי $p|q_j$.

נוכיח עבור $n+1$. נתון $p|q_1\cdot q_2\cdot\ldots\cdot q_n\cdot q_{n+1}$, לא ידוע לנו אם $p|q_1\cdot q_2\cdot\ldots\cdot q_n$ אך אם הוא כן סיימנו לפי הנחת האינדוקציה. לכן נניח כי $p\nmid q_1\cdot q_2\cdot\ldots\cdot q_n$, ואזי ה-gcd שלהם יהיה 1. לפי משפט (2) ב-gcd מכיוון ש-$p|(q_1\cdot q_2\cdot\ldots\cdot q_n)\cdot q_{n+1}$ וגם מתקיים $(p,(q_1\cdot q_2\cdot\ldots\cdot q_n))=1$, אזי $p|q_{n+1}$. ולכן בכל מקרה קיים $j\in[n+1]$ כך ש-$p|q_j$.

הוכחת המשפט היסודי: נוכיח קיום ויחודיות בשתי דרכים W.O.P ואינדוקציה.

W.O.P - (1) קיום - נניח כי הטענה אינה נכונה וכי קיימת קבוצה של מספרים שלמים הגדולים מ-1 שלא ניתן להציג אותם כמכפלה של ראשוניים. לפי ההנחה ועקרון W.O.P קיים איבר מינימלי בקבוצה זו, יהי זה n. n אינו ראשוני שכן אחרת הוא לבדו מקיים את המשפט, לכן n פריק. אם כך קיימים $a,b\in Z$ כך ש-$2\leq a,b<n$ המקיימים $n=a\cdot b$. היות ו-n הוא

21/11

בס"ד

האיבר המינימלי שלא ניתן להציג כמכפלת ראשונים ו- $a,b<n$. אזי את a,b כן ניתן להציג כמכפלת ראשונים, ומתוך כך גם את n. סתירה! מכאן שכל מספר שלם הגדול מ-1 ניתן להציג כמכפלת ראשוניים.

יחידות- נניח בשלילה כי קיים מספר שלם $n>1$ שניתן להציג אותו בשתי מכפלות ראשוניים שונים: $n=q_1\cdot q_2\cdot\ldots\cdot q_n=p_1\cdot p_2\cdot\ldots\cdot p_m$. נניח כי אין מספרים זהים בין $q_1,q_2,\ldots,q_n$ ו-$p_1,p_2,\ldots,p_m$ משום שאם אכן היה יכולנו לצמצם אותם. היות ומתקיים: $p_1(p_2\cdot p_3\cdot\ldots\cdot p_m)=q_1\cdot q_2\cdot\ldots\cdot q_n$ אזי $p_1|q_1\cdot q_2\cdot\ldots\cdot q_n$. לפי המשפט עזר קיים $j\in[n]$ כך ש-$p_1|q_j$ ומכיוון ששניהם ראשוניים אזי הם גדולים מ-1 ומתקיים $p_1=q_j$, שזה סתירה לכך שאין גורמים משותפים בין הייצוגים. מכאן שלא יכולים להיות שני ייצוגים של מכפלת ראשוניים לאותו מספר.

אינדוקציה (2) קיום- בסיס- עבור $n=2$ הטענה נכונה כי 2 לבדו מקיים את המשפט.

צעד- נניח כי הטענה נכונה עבור כל המספרים $n\geq k>1$, שניתן להציגם כמכפלת ראשוניים נוכיח עבור $n+1$. אם $n+1$ ראשוני אזי הוא לבדו מקיים את המשפט, לכן נניח ש-$n+1$ פריק. אם כך קיימים $a,b\in Z$ כך ש-$2\leq a,b<n+1$ המקיימים $n+1=a\cdot b$. מכיוון ש-$n+1>a$ ולפי הנחת האינדוקציה ניתן לפרק את a ו-b כמכפלת ראשוניים, ומתוך גם את n.

יחודיות- בסיס- עבור $n=2$ הטענה נכונה כי אין ראשוני קטן ממנו.

צעד- נניח כי הטענה נכונה עבור כל המספרים $1<k\leq n$ שיש להם מכפלת ראשוניים יחודית נוכיח עבור $n+1$. כבר הוכחנו שקיימת מכפלה של ראשוניים המבטאים את $n+1$. נניח כי קיימים שני ייצוגים אפשריים ל-$n+1$. $n+1=q_1\cdot q_2\cdot\ldots\cdot q_s=p_1\cdot p_2\cdot\ldots\cdot p_m$

כמו בהוכחה ב-W.O.P נניח כי אין מספרים זהים בין הייצוגים. היות ומתקיים: $p_1(p_2\cdot p_3\cdot\ldots\cdot p_m)=q_1\cdot q_2\cdot\ldots\cdot q_s$ אזי $p_1|q_1\cdot q_2\cdot\ldots\cdot q_s$. לפי המשפט עזר קיים $j\in[s]$ כך ש-$p_1|q_j$ ומכיוון ששניהם ראשוניים הגדולים מ-1 $p_1=q_j$. כעת אפשר לצמצם שני גורמים אלו ולקבל מספר קטן יותר מ-$n+1$. לפי הנחת האינדוקציה למספר זה מכפלת ראשוניים יחודית, כך שנדע שכל האיברים בשתי ההצגות שווים. ומכאן שכל האיברים בשתי ההצגות של $n+1$ שווים, ולכן ל-$n+1$ יש מכפלת ראשוניים יחודית.א.

21/11

בס"ד

מספרים ראשוניים

א) מוטיבציה

בפרק זה נעסוק בכמות המספרים הראשוניים הקיימים, חלוקה שלהם ומשפטים חשובים נוספים. המוטיבציה שלנו בפרק זה הוא שבמדעי המחשב פוגשים סדרות רבות באופן טבעי דרך ניתוח לולאות. העובדה לגבי סדרות אלו שיש איזשהו חוק שניתן למצוא בקלות כל איבר במקום ה-i שנרצה. לעומת זאת בסדרת המספרים הראשוניים $p_1,p_2,\dots,p_n$ האנושות עדיין לא הצליחה למצוא איזה חוק פשוט ומהיר למצוא כל מספר ראשוני במקום ה-i. לכן העיסוק בסדרה זו יש לו משמעות גדולה בתחום המתמטיקה, סייבר ועוד.

ב) משפט אוקלידס

משפט אוקלידס חלק 1: יש אינסוף מספרים ראשוניים.

הוכחה: נניח בשלילה שיש מספר סופי של ראשוניים שהם $p_1,p_2,\dots,p_n$ קבוצת כל הראשוניים הקיימים. נגדיר מספר Q כך ש- $Q=p_1\cdot p_2\cdot\ldots\cdot p_n+1$. מכיוון ש-$Q>p_n$ הוא אינו ראשוני אלא פריק, כך שקיים לו מחלק ראשוני q. מכיוון ש-q ראשוני מתקיים $q|p_1\cdot p_2\cdot\ldots\cdot p_n$ ולפי הגדרת q גם מתקיים $q|p_1\cdot p_2\cdot\ldots\cdot p_n+1$. לפי משפט (2) במשפט החלוקה נמצא כי $q|p_1\cdot p_2\cdot\ldots\cdot p_n+1-p_1\cdot p_2\cdot\ldots\cdot p_n=1$, ולכן $q=1$. שזו סתירה שהרי הגדרנו q ראשוני.
נמצא כי לא ניתן להגדיר קבוצה סופית של ראשוניים.

משפט אוקלידס חלק 2: בסדרת המספרים הראשוניים לכל $n\ge1$ מתקיים: $p_{n+1}\le p_1\cdot p_2\cdot\ldots\cdot p_n+1$

הוכחה: נגדיר $Q=p_1\cdot p_2\cdot\ldots\cdot p_n+1$. אם Q ראשוני אז בוודאי ש- $p_{n+1}\le Q$, כי $p_n<Q$ ולפי הגדרת הסדרה מובטח לנו שאין ראשוניים בין p_n ל- p_{n+1}. לפיכך נניח כי Q אינו ראשוני אלא פריק, כך שיש לו מחלק ראשוני q. אם $q\ge p_n$ אז שוב בוודאי $p_{n+1}<Q$ שהרי $Q>q$. לכן נניח כי $q\le p_n$. אם כן נמצא ש-$q|p_1\cdot p_2\cdot\ldots\cdot p_n$, ואז כמו בחלק 1 של המשפט יוצא ש- $q=1$ שזו סתירה להגדרת q ראשוני.
נמצא שגם אם Q ראשוני או ש- $q>p_n$, בשני המקרים $p_{n+1}\le Q$.

28/11

בס"ד

א) צורות אינסוף ראשוניים

(1) **משפט:** יש אינסוף ראשוניים מהצורה $4n+3$. לפני הוכחת משפט זה נלמד משפט עזר:

משפט עזר: מכפלת k מספרים מהצורה $4n+1$ נשארת בצורה זו. משפט עזר

הוכחה: $(4n+1)(4m+1)=16mn+4m+4n+1=4\cdot4mn+4\cdot m+4\cdot n+1=4(4mn+m+n)+1 \Rightarrow$ מ.ש.ל.

ניסיון הוכחה כושל: ננסה להוכיח באותה טכניקה של משפט אוקלידס חלק ד. נניח בשלילה כי קיים מספר סופי של ראשוניים מהצורה $4n+3$, ומספרים אלו יהיו הקבוצה: $P_1,P_2,P_3,\dots,P_n$
$3 \neq 11$
נגדיר Q כך ש-$Q=4(P_1\cdot P_2\cdot\ldots\cdot P_n)+3$. מכיוון ש-$Q>P_n$ ו-Q מהצורה $4n+3$ Q אינו ראשוני. ולכן Q פריק כך שיש לו מחלק ראשוני q. ננסה להראות ש-q מהצורה $4n+3$ אך $q\notin S$, ובכך להגיע לסתירה. Q הוא מהצורה $4n+3$ כלומר איננו זוגי ולכן $q\neq2$. מכיוון ש-q ראשוני וכל ראשוני חוץ מ-2 הוא אי זוגי, וכן מכיוון שכל מספר אי זוגי הוא מהצורה $4n+3$ או $4n+1$, אזי גם q הוא אחד מצורות אלו. לפי המשפט עזר אזי בגלל ש-Q מהצורה $4n+3$ לא יכול להיות שכל המחלקים שלו מהצורה $4n+1$ כי אחרת גם הוא היה מצורה זו. לכן ל-Q יש מחלק ראשוני שהינו מהצורה $4n+3$, יהי זה q. נמצא ש-$q\mid P_1\cdot P_2\cdot\ldots\cdot P_n$ ואזי גם $q\mid 4\cdot P_1\cdot P_2\cdot\ldots\cdot P_n$, וכן $q\mid Q$. מכאן לפי משפט (2) במשפט החלוקה $q\mid Q-4\cdot P_1\cdot P_2\cdot\ldots\cdot P_n=3$. לא הצלחנו להגיע לסתירה כי יכול להיות $q=3$.

ניסיון הוכחה נוסף: נשים לב כי הקבוצה $4n+3$ זהה לקבוצה $4n-1$ (ניתן להוכיח בהכלה דו כיוונית) $\{4n+3:n\in\mathbb{Z}\}=\{4n-1:n\in\mathbb{Z}\}$. לכן ננסה להוכיח שיש אינסוף ראשוניים מהצורה $4n-1$. נשתמש באותה דרך הוכחה כמו בניסיון הקודם, אלא שנגדיר $Q=4(P_1\cdot P_2\cdot\ldots\cdot P_n)-1$. נבצע את אותן פעולות כמו בניסיון הקודם כך שנקבל: $q\mid Q-4\cdot P_1\cdot P_2\cdot\ldots\cdot P_n=-1$. שזו סתירה, שהרי הגדרנו q ראשוני שונה מ-2 ולכן $q\geq3$. נמצא שלא ניתן להגדיר קבוצה עם מספר סופי של ראשוניים מהצורה $4n+3$. מ.ש.ל.

(2) **משפט דיריכלה (Dirichlet)** - יהיו a,b שני מספרים שלמים גדולים מ-0, $a,b\in\mathbb{Z}^+$, אזי אם $(a,b)=1$ אז בסדרה מהצורה $an+b$ יש אינסוף ראשוניים.

הוכחת משפט זה לא כלולה בחומר של הקורס.

28/11

בס"ד

3) משפטים

(1) **משפט בונזה (Bonse):** לכל $n\geq 5$ מתקיים: $(p_{n+1})^2 < p_1\cdot p_2\cdot\ldots\cdot p_n$

הוכחה לא במסגרת הקורס

(2) **משפט:** לכל $n\geq 1$ מתקיים: $p_n \leq 2^{2^n}$

הוכחה: באינדוקציה על n.

בסיס- עבור $n=1$ נקבל $p_1 = 2 \leq 2^{2^1} = 4$ ✓

צעד- נניח כי הטענה נכונה עבור $1\leq k\leq n$ $p_n \leq 2^{2^n}$

נוכיח עבור $n+1$. לפי משפט אוקלידס: $p_{n+1} \leq p_1\cdot p_2\cdot\ldots\cdot p_n+1$

נפעיל את הנחת האינדוקציה לכל אחד מהראשונים עד n: $p_{n+1} \leq 2^{2^1}\cdot 2^{2^2}\cdot\ldots\cdot 2^{2^n}+1 = 2^{2^1+2^2+\ldots+2^n}+1 =$

בתרגול אינדוקציה הוכחנו: $\sum_{i=1}^{n} 2^i \leq 2^{n+1}-1$ $= 2^{\sum_{i=1}^{n} 2^i}+1 \leq 2^{2^{n+1}-1}+1$

מספר זה קטן מהכפולה ב-2 ולהוריד 1: $\leq 2\cdot 2^{2^{n+1}-1} = 2^{2^{n+1}} \Rightarrow$ מ.ש.ל.

(3) **משפט:** עבור $n\geq 1$ קיימים לפחות n ראשוניים קטנים מ- 2^{2^n}.

הוכחה: לפי משפט (2) $p_n\leq 2^{2^n}$ לכן ישנם לפחות n ראשוניים $p_1,p_2,\ldots,p_n$ הקטנים מ- 2^{2^n}.

(4) **משפט ברטרנד (Bertrand):** לכל $n\geq 2$ ישנו לפחות ראשוני אחד באינטרוול הפתוח $(n,2n)$.

הוכחת משפט זה איננה במסגרת הקורס

(5) **משפט:** עבור $n\geq 2$ מתקיים: $p_{n+1}<2p_n$.

הוכחה: לפי משפט ברטרנד באינטרוול הפתוח $(p_n, 2\cdot p_n)$ יש לפחות ראשוני אחד שאיננו $2\cdot p_n$ או p_n. לכן $p_{n+1}<2\cdot p_n$.

(6) **משפט:** עבור $n\geq 2$ מתקיים $p_n\leq 2^n$.

הוכחה: באינדוקציה על n.

בסיס- עבור $n=2$ נקבל: $p_2=3\leq 2^2=4$ ✓

צעד- נניח כי הטענה נכונה עבור $1\leq k\leq n$ $p_n\leq 2^n$.

נוכיח עבור $n+1$. לפי משפט ברטרנד האינטרוול הפתוח $(2^n, 2^{n+1})$ מכיל לפחות ראשוני אחד, יהי זה q. נמצא שמתקיים $2^n<q<2^{n+1}$, ולפי הנחת האינדוקציה $p_n<2^n<q<2^{n+1}$

מכיוון שלפי הגדרת הסדרה אין ראשוניים בין p_n ל- p_{n+1} מחייב שמתקיים $p_{n+1}\leq q$

אזי $p_{n+1}<2^{n+1}$ מ.ש.ל. נמצא שאכן הוכחנו $p_n<2^n$ שבו טענה חזקה יותר ממשפט 2

Scanned with CamScanner