נאמר את המשפט בלי הוכחה וכלל לגבל:

③ אם רוצים למצוא ∞ פתרונות, הם כולם מהצורה

$x = x_0 + \left(\frac{b}{d}\right)t \qquad y = y_0 - \left(\frac{a}{d}\right)t$ לכל $t\in\mathbb{Z}$

(מי שרוצה הוכחה יש בספר הקורס שבמודל).

מספרים ראשוניים

הגדרה: מספר $1<a\in\mathbb{N}$ נקרא ראשוני אם הוא מתחלק רק בעצמו וב-1.

מספר שאינו ראשוני נקרא פריק.

1 - לא ראשוני, 2 - ראשוני, 7 - ראשוני, 9 - לא ראשוני.

המשפט היסודי של האריתמטיקה: "כל טבעי יש פירוק יחיד לראשוניים" לדוג': $24=2\cdot2\cdot2\cdot3 = 2^3\cdot3$ (צורה קנונית)

כל טבעי גדול מ-1 ניתן להצגה כמכפלת ראשוניים. ההצגה יחידה (הסבר מיון) עד כדי סדר האיברים.

צורה קנונית של פירוק לראשוניים: $n=p_1^{a_1}\cdot p_2^{a_2}\cdots p_k^{a_k}$, $a_i>0$ $\forall i\in[k]$, $\underbrace{p_1<\dots<p_k}_{\text{נקראים "איברים ראשוניים"}}$

(נפתח טפה את הוכחת המשפט היסודי כדי להוכיח כמה הבנות)

למה: לכל $n>1$ טבעי יש מחלק ראשוני. (זו גרסה התחלתית חלשה מאשר המשפט היסודי).

הוכחה: נניח בשלילה שלא ויהי n הטבעי הקטן ביותר שאין לו מחלק ראשוני. (שמש בסדר טוב!). אם n ראשוני אז הוא מחלק עצמו. אם n פריק אז $n=a\cdot b$ עבור $2\le a,b<n$, ומהמינימליות של n יש ל-a מחלק ראשוני p ⇐ חלק, סתירה.

מסקנה: אם $n>1$ פריק אז יש לו מחלק ראשוני $\le\sqrt{n}$. (כי אחרת, נקבל כהוכחה הקודמת $a,b>\sqrt{n}$ ⇐ $n<a\cdot b$.)

אמת/שקר: אם p ראשוני ו-$p|ab$ אז $p|a$ או $p|b$ (אם p לא ראשוני זה לא נכון $12|6\cdot4$ אבל $12\nmid6$, $12\nmid4$; $6=2\cdot3$, $4=2\cdot2$)

אמת!

תזכורת: הלמה של אוקלידס "אם מספר מחלק מכפלת שני מספרים וזר לאחד מהם, אז הוא מחלק את השני".

הוכחה: אם $p|a$ סיימנו. אחרת $(p,a)=1$, ואז לפי הלמה של אוקלידס $p|b$.

כי עבור ראשוני $(p,\square)$ האפשרויות 1 או p

הכללה:

"אם ראשוני p מחלק מכפלה, אז הוא מחלק את אחד האיברים"

אם p ראשוני ו-$p|a_1\cdots a_n$ ($\forall i\in[n], a_i>0$)

אז קיים $j\in[n]$ כך ש-$p|a_j$.

לא ראשוני, ולכן גורם אחד שלו הגיע מ-9 והשני מ-2. אבל בראשוני זה לא קורה

$6|9\cdot2\cdot2$ ($6=3\cdot2$, $9=3\cdot3$, 2, 2)

<u>הוכחה:</u> (אינדוק' על k)

בדיקה עבור $k=1$: ✓

נניח נכונות עבור k (כלומר: מניחים שאם p מחלק מכפלה של k אז הוא מחלק את אחד הגורמים)

נוכיח עבור k+1: אם $p \mid \underbrace{(a_1 \cdots a_k)}\underbrace{a_{k+1}}$ אז p מחלק את אחד הגורמים.

אכן, [אינטואיציה: אם p מחלק את ( ) אז הוא מחלק את אחד הגורמים מה"א. אחרת p לא מחלק את ( ) ולפי למת גאוס/שפר מפריט קודם $p \mid a_{k+1}$
לשים לב לצורך של הפיכת המכפלה למכפלה של שניים!)]

אם $p \mid a_1 \cdots a_k$ אז מה"א $p \mid a_j$ עבור איזה $1 \le j \le k$

ואם $p \nmid a_1 \cdots a_k$ אז מהטענה הקודמת נקבל $p \mid a_{k+1}$.

<u>מסקנה:</u> אם $p \mid q_1 \cdots q_n$, $q_1, \dots, q_n$ ראשוניים אז קיים $1 \le j \le n$ כך ש $p = q_j$. (כי לפי ההכללה יש j כך ש- $p \mid q_j$, ומראשוניות q_j נקבל $q_j = p$).

<u>הוכחת המשפט היסודי של האריתמטיקה:</u>

<u>קיום:</u> נניח בשלילה שהטענה לא נכונה, ויהי n הטבעי הקטן ביותר שלא ניתן להצגה כמכפלת ראשוניים. (קיים לפי WOP). ברור ש-n אינו ראשוני ולכן n פריק כלומר $n = ab$, $2 \le a, b < n$, אבל ממינימליות n, a ו-b כן ניתנים להצגה כמכפלת ראשוניים ולכן גם $n = a \cdot b$ ניתן להצגה כמכפלת ראשוניים, סתירה.

<u>יחידות:</u> נניח בשלילה שיש ל-n שני פירוקים שונים לראשוניים
$n = p_1 \cdots p_s = q_1 \cdots q_l$, בה"כ שם p_1 אינו שווה לאף q_j.
(כי ניתן להניח שצמצמנו גורמים ראשוניים משותפים). להסביר!

נקבל כי $p_1 \mid q_1 \cdots q_l$ ומהמסקנה נקבל $p_1 = q_j$ לאיזה $1 \le j \le l$, סתירה.

<u>שימושים למשפט היסודי:</u>

① איך נדע אם מספר מחלק מספר אחר? ע"י פירוק לראשוניים בצורה הקנונית

האם $\underset{2^3 \cdot 3 \cdot 5}{\overset{\shortparallel}{120}} \mid \underset{2^2 \cdot 5}{\overset{\shortparallel}{20}}$ ✓ כל גורם ראשוני משותף מופיע גם מימין עם חזקה גדולה או שווה.

האם $\underset{2^3 \cdot 3 \cdot 5}{\overset{\shortparallel}{120}} \mid \underset{2^4}{\overset{\shortparallel}{16}}$ לא! כי החזקה של הגורם הראשוני 2 משמאל גדולה יותר.

<u>אבחנה:</u> אוסף המחלקים של $\prod_{i=1}^{r} p_i^{a_i} = \underbrace{n = p_1^{a_1} \cdots p_r^{a_r}}_{\text{פירוק קנוני לראשוניים}}$ הוא

$$\left\{ \prod_{i=1}^{r} p_i^{c_i} \mid 0 \le c_i \le a_i \right\}$$

② איך נמצא gcd בלי האלגוריתם של אוקלידס?

$$(2100, 720) = ?$$

(אין מונחים! מחלקים ב-2 כל אחד ובסוף ואחד ב-3 ואחד ב-5 וכו')

$$720 = 2^4 \cdot 3^2 \cdot 5 \qquad 2100 = 2^2 \cdot 3 \cdot 5^2 \cdot 7$$

(והשל כאן 7^0)

$$= 2^2 \cdot 3 \cdot 5 \overset{\text{והשל } 7^0}{\cdot} = 60$$

אבחנה: אם
$$\begin{cases} a = p_1^{a_1} \cdot \ldots \cdot p_n^{a_n} \\ b = p_1^{b_1} \cdot \ldots \cdot p_n^{b_n} \end{cases}$$
כאשר p_i ראשוניים $b_i, a_i \geq 0$

(בתיראולים תקראו לזה ספלורצת)

כאן חזקה שיפוח כבה אמת גרסה
גם אם מספר ... 0, לכלל - כבדה
וכל ש משמש $7^0 = 1$

$$(a,b) = p_1^{\min\{a_1, b_1\}} \cdot \ldots \cdot p_n^{\min\{a_n, b_n\}}$$ אז

אינסופיות הראשוניים

כבר אוקלידס, בספרו "היסודות" ידע להוכיח שיש ∞ ראשוניים. (נסו לחשוב על הוכחה!)
(זוהי היא את ההוכחה הראשונה של הוכחה בשלילה)

משפט (אוקלידס): יש ∞ ראשוניים. (רעיון ההוכחה - אם יש מספר סופי - כל הראשוניים עד אפשר לבנות ראשוני)

הוכחה: נניח בשלילה שיש רק כמות סופית של ראשוניים והם $p_1, \ldots, p_n$.

ויהי $Q = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$

לפי הלמה מתחילת ההרצאה (כל מספר >1 יש מחלק ראשוני) יש ל-Q מחלק ראשוני, והוא בהכרח אחד p_i עבור $n \geq i \geq 1$ כלשהו.

לכן $p_i | Q \Leftarrow p_i | \underbrace{Q - p_1 \cdot \ldots \cdot p_n}_{1} \Leftarrow p_i | 1$ סתירה.

כי p_i מחלק גם את Q וגם את $p_1 \cdot \ldots \cdot p_n$

מש"ל

מסקנה שנובעת מהמשפט: אם $p_1, \ldots, p_n$ הם n הראשוניים הראשונים אז למספר $p_1 \cdot \ldots \cdot p_n + 1$ יש מחלק ראשוני שאינו אחד מבין $p_1, \ldots, p_n$. כלומר הראשוני הבא בתור אחרי p_n הוא בהכרח $\leq p_1 \cdot \ldots \cdot p_n + 1$

הוכחה נוספת שיש ∞ ראשוניים: בתרגול 4 הכרנו את מספרי פרמה $F_n = 2^{2^n} + 1$ וראינו שכל שניים זרים זה לזה. לכן בכל מס' פרמה יש גורם ראשוני שלא מופיע באחרים ולכן עד F_n (כולל) יש לפחות n ראשוניים כלומר $p_n \leq F_n = 2^{2^n} + 1$.

(p_n - הראשוני ה-n-י)

כל מה שרציתם לדעת על ראשוניים ולא העזתם לשאול:

* העיקרון האסימפטוטי: עד n יש בערך $\frac{n}{\log n}$ ראשוניים.
זה הוכח בסוף המאה ה-19 ע״י פונקציות מרוכבות (באופן מפתיע, כדי להוכיח טענה על מספרים טבעיים נדרשו כלים כבדים כמו מספרים מרוכבים!)
והוכח שוב באמצע המאה ה-20 ע״י ארדש וסלברג בכלים אלמנטריים.

* הפוסטולט של ברטרנד: לכל $n \geq 2$, יש בקטע הפתוח $(n,2n)$ לפחות
משהו בין השערה למשפט
ראשוני אחד.

ברטרנד ישער את זה ב-1845, צ׳בישב הצליח להוכיח ב-1852, ובמאה ה-20 ארדש הוכיח בכלים פשוטים יותר, וחיבר שיר לכבוד ההישג:

Tchebycheff proved it, I proved it again:
There is always a prime between 2n and n.

* השערת גולדבך: כל מספר זוגי אפשר לרשום כסכום של שני ראשוניים.
לדוגמה: $16 = 11+5$
ההשערה פתוחה עד היום!

* מי שיצליח לפתור את התרגיל הבא, יקבל ציון 100 בקורס (ולא משנה מה ציון המטלות שלו):
תרגיל: הוכח שיש אינסוף זוגות של ראשוניים מהצורה $(n,n+2)$.
(כגון $(5,7)$, $(11,13)$, $(29,31)$, ...)

מספרים א"ז (מתחלקים לשני סוגים)

$\{4n+1 \mid n\in\mathbb{Z}\}$

אבחנה: מכפלת שניים כאלו גם היא מהצורה $4n+1$

(בדקה.)

$$(4n+1)(4m+1) = \underbrace{16mn+4n+4m+1}_{4(4mn+n+m)+1}$$

באינדוקציה נובע שגם מכפלה סופית של כאלו היא גם מאותה צורה.

$\{4n+3 \mid n\in\mathbb{Z}\} = \{4n-1 \mid n\in\mathbb{Z}\}$

מכפלת שניים כאלו היא מהצורה $4n+1$ (בדקו)

ראינו שיש ∞ ראשוניים ומלבד 2 כולם א"ז. האם יש ∞ מכל אחת משתי הצורות? או רק מאחת מהן? מסתבר שיש ∞ משני הסוגים.

טענה: יש ∞ מספרים ראשוניים מהצורה $4n+3$.

נסיון הוכחה כושל (הערה): (מנסים לחקות את הוכחת אוקלידס לקיום ∞ ראשוניים - ואין זו הדרך התמימה שמתמטיקאי ינסה, לחקות הוכחה של טענה דומה.)

נניח בשלילה שיש מס' סופי של ראשוניים מהצורה $4n+3$, ונניח שהם $3,7,\dots,p$

נגדיר

$$Q = 4\cdot(3\cdot 7\cdot\ldots\cdot p)+3$$

(ולא ישירות $Q=3\cdot 7\cdot\ldots\cdot p+3$ כי אז ברור שלא יצא משהו מהצורה $4n+3$)

לפי הלמה מתחילת ההרצאה (לכל מס' >1 יש מחלק ראשוני) יש ל-Q מחלק ראשוני, ולפי האבחנה בכיוון ההפוך יש ל-Q מחלק ראשוני מהצורה $4n+3$ (אחרת, אם כל מחלקי Q מהצורה $4n+1$ היה נובע כי גם Q מהצורה הזו והוא לא.)

כאן היינו רוצים להגיע לסתירה, אבל דווקא לא - אין 3 מחלק כזה ואין סתירה.

(זה עוד לא אומר שהטענה שגויה או שאי אפשר להמשיך ולנסות בכיוון הזה... אבל אנחנו נפנה לכיוון אחר.)

ננסח את הטענה באופן שקול:

טענה: יש ∞ ראשוניים מהצורה $4n-1$

הוכחה: נניח בשלילה יש מס' סופי של ראשוניים מהצורה $4n-1$ ונניח שהם $3,7,\dots,p$.

יהי

$$Q = 4(\underbrace{3\cdot 7\cdot\ldots\cdot p}_{\text{כל הראשוניים מהצורה } 4n-1})-1$$

לפי הלמה הנ"ל יש ל-Q מחלק ראשוני, ולפי האבחנה יש ל-Q מחלק ראשוני q מהצורה $4n-1$.

אז $q \mid Q$ וגם $q \mid (\underbrace{3\cdot 7\cdot\ldots\cdot p}_{\text{כי מופיע ברשימה}})$ $\Leftarrow$ $q \mid Q-4\cdot(3\cdot 7\cdot\ldots\cdot p) = -1$ $\Leftarrow$ סתירה.

שאלה למחשבה לקראת התרגול: עכשיו כשראינו שעובדת ההוכחה עם "$4n-1$", תחשבו מדוע אין האבחנה הנ"ל עובדת ואיך לשנות את ההוכחה כדי להצליח. (רמז: $Q=4(7\cdot\ldots\cdot p)+3$)

למעשה, יש מהצורה הזאת יש ∞ ראשוניים, אבל את זה הרבה יותר קשה להוכיח. זה נובע ממשפט דיריכלה.

<u>משפט דיריכלה</u> (Dirichlet's Theorem):

אם $(a,b)=1$ אז בסדרה החשבונית $\{an+b \mid n\in\mathbb{N}\}$ יש ∞ ראשוניים.

<u>לדוגמה</u>: $a=4$
$b=1$

$$\{an+b \mid n\in\mathbb{N}\} = \{5, 9, 13, 17, 21, \ldots\}$$

מס' מהצורה $4n+1$ ולפי המשפט יש ∞ ראשוניים מהצורה $4n+1$.

(זוהי סדרה חשבונית כי ההפרש קבוע)

סוף הרצ. 5