משפט היסודי של האריתמטיקה:
כל מספר שלם גדול מ-1 ניתן להצגה בצורה **יחידה** ע"י
מכפלה של גורמים ראשוניים באופן הבא:

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

כאשר לכל $i\in[k]$ אזי p_i ראשוני
$a_i \geq 0$
וגם $p_1<p_2<\ldots<p_k$

הוכחה: יש צורך להראות קיום ויחידות.
קיום: נניח בשלילה כי הטענה אינה נכונה ולכן קיימת קב' של מספרים חיוביים שלא ניתנים להצגה ע"י מכפלה של גורמים ראשוניים, יהא n הדוגמא הנגדית המינימלית.
אם n ראשוני אזי n מוצג בצורה עצמית כי $n=n$
ראשוני
אם n לא ראשוני אזי הוא 1 או מספר פריק. 1 לא נכלל שהרי כי מדובר על שלמים >1
ולכן n פריק. לפי הגדרה, $\exists a,b$ כך ש $n=a\cdot b$
וגם $a,b\in[2,n-1]$. והמספרים a,b **אינם** דוגמאות נגדיות היות
וגם הם קטנים אזי יש סתירה למינימליות של n, ולכן
ניתן להציג את a,b ע"י מכפלה של גורמים ראשוניים
באופן הבא:

$$a=p_1^{a_1}\cdots p_s^{a_s}$$
$$b=q_1^{b_1}\cdots q_k^{b_k}$$

ולכן $n=a\cdot b=\prod_{i=1}^{s}p_i^{a_i}\prod_{i=1}^{k}q_i^{b_i}$

ולכן השגנו סתירה.

יחידות: נניח בשלילה ש $p_1^{a_1}\cdots p_k^{a_k} = n = q_1^{b_1}\cdots q_\ell^{b_\ell}$
אם יש בשני הצדדים גורמים ראשוניים משותפים, אז נצמצם אותם. ולכן נניח כי יש גורמים ראשוניים זרים בב' הצדדים.
הבחנו כי $p_1^{a_1}\cdots p_k^{a_k} = q_1^{b_1}\cdots q_\ell^{b_\ell} \Rightarrow p_1^{a_1}\mid q_1^{b_1}\cdots q_\ell^{b_\ell}$
ולכן קיים $j\in[\ell]$ כך ש $p_1\mid q_j$ ולכן $p_1=q_j$
בסתירה לכך שהם היו המצומצמים ביותר בשני הצדדים

מה ידוע לנו עד כה לגבי ראשוניים (בסכמה)?

* מספר ראשוני - מספר שמתחלק רק ב-1 ובעצמו —
* כל מספר שגדול > 1 ניתן להציג בצורה יחידה ע"י מכפלה של ראשוניים (המשפט היסודי של האריתמטיקה)
* כל מספר שגדול > 1 מתחלק בראשוני (כלשהו) בהוכחה.
* לכל מספר פריק n קיימים $a,b\in[2,n-1]$ כך ש $n=a\cdot b$
* לכל מספר פריק n קיים גורם ראשוני עד $\sqrt{n}$.
* יש ∞ ראשוניים בסה"כ (הוכח בהרצאה)
* $\forall a,b\in\mathbb{Z}$ כך ש $p|ab$ אזי $p|a$ או $p|b$.

<u>תרגיל:</u> $\forall a,b\in\mathbb{Z}$ כך ש $p|ab$ אז $p|b \underset{\text{או}}{\vee} p|a$

<u>הוכחה:</u> ידוע ש $p|ab$.

אם $p|a$ סיימנו

אם $p\nmid a$ אזי $(p,a)=1$ ולכן לפי הלמה (*)

$p|b$

(*) תזכורת מתמטיקה: אם $a|bc$ ו $(a,b)=1$ אזי $a|c$.

<u>תרגיל:</u> $\sqrt{p}$ אי רציונלי כאשר p ראשוני כלשהו

נניח בשלילה ש $\sqrt{p}\in\mathbb{Q}$ ולכן $\sqrt{p}=a/b$ כאשר $a,b\in\mathbb{Z}$

ונבחר אותם שהיו המצומצמים ביותר, ולכן נניח ש $(a,b)=1$

כי אם לא, אז פשוט נצמצם עד שנגיע לצורה.

$\sqrt{p}=a/b \Rightarrow a=\sqrt{p}\cdot b \Rightarrow a^2=pb^2$

ולכן $p|a^2$ ולכן $p|a$ לפי השאלה הקודמת.

ומכן לפי הגדרה $a=p\cdot k,\ k\in\mathbb{Z}$ ולכן

$a^2=pb^2$

$p^2k^2=pb^2$

$pk^2=b^2 \underset{\text{אותה סיבה}}{\Rightarrow} p|b \Rightarrow (a,b)=p\geq 2 \neq 1$

<u>בסתירה להנחה!</u>

תרגיל: הוכיחו כי יש ∞ ראשוניים ע"י שימוש ב N
$n!+1$ (ההוכחה שראינו בשיעור הייתה עם $\prod_{i=1}^{n} p_i + 1$)

הוכחה: נניח בשלילה שקיימת רק סופית של ראשוניים בעולם.
ונגדיר $S=\{p_1 \dots p_n\}$ שהיא קבוצת כל הראשוניים.
נסמן ב q שהוא הראשוני הגדול ביותר בקבוצה S.
נגדיר $N=n!+1$ כאשר $n>q$.
נשים לב כי $n>q\geq 2$ ולכן $N>1$
ולכן קיים ל N גורם ראשוני כלשהו, נקרא לו p.
ונדע כי $p|N$ ובנוסף $p|n!$ כי p נמצא
במכפלה של $1\cdot 2\cdots p\cdots n$ כי $q<n$ ו q הוא
הראשוני הגדול ביותר. ולכן מכנה מסוקה, $p|N-n!=1$
אבל זה לא יכול להיות, היות ו $p\geq 2$.

תרגיל: 1. כל מספר ראשוני מהצורה $3n+1$ הוא גם מהצורה $6m+1$
2. לכל מספר שלם מהצורה $3n+2$
קיים מחלק ראשוני מאותה צורה
3. המספר הראשוני היחיד מהצורה n^3-1 הינו 7.

1. יהי $p=3n+1$ עבור $n\in\mathbb{Z}$. נראה כי $p=6m+1$ בהכרח.
לפי משפט החלוקה, כל מספר שלם ניתן לרשום באחת מהצורות הבאות: $6m, 6m+1, 6m+2, 6m+3, 6m+4, 6m+5$
היות ו-p ראשוני אזי הוא אינו יכול להיות
באחת מהצורות הבאות:

$$6m = 2(3m)$$
$$6m+3 = 3(2m+1)$$
$$6m+2 = 2(3m+1)$$
$$6m+4 = 2(3m+2)$$

ולכן נותר רק הצורות $6m+1$, $6m+5$.
נניח ו-p מהצורה $6m+5$
ולכן $6m+5 = 3n+1$

$$3(2m-n) = 4$$
$$2m-n = 4/3 \notin \mathbb{Z}!$$

ולכן נותר רק $6m+1$!

2. יהי $p=3n+2$ עבור $n\in\mathbb{Z}^+$

נניח בשלילה כי ל-p אין מחלק מהצורה $3k+2$

ולכן כל המחלקים מהצורה $3k$ או $3k+1$.

נשים לב כי לצורה $3k$ נפסלת היות

וזה לא ייתכן שהרי (p ראשוני)

ולכן כל המחלקים של p מהצורה $3k+1$

נשים לב כי מכפלה של שני מספרים מהצורה

$3k+1$ נשארת בצורה זו היות ו:

$$(3k+1)(3m+1)=9km+3k+3m+1=3(3km+k+m)+1$$

אבל p מהצורה $3n+2$ ולכן חייב שיש גורם אחר

חוץ מ $3k+1$.

<u>תרגיל בית</u>: הוכיחו כי כל מספר ~~p~~ ק/[illegible] מהצורה $4n+3$

מכיל לפחות מחלק אחד מהצורה $4m+3$.

3. נשים לב כי

$$n^3-1=(n-1)(n^2+n+1)$$

ולכן $n=2$ בהכרח כדי ש p יהיה ראשוני

ולכן נקבל כי $p=7$.