מרצה: ד"ר אלעד חורב

להערות/הארות/תיקונים - נעם דומוביץ - $ndomovich@gmail.com$

תורת המספרים האלגוריתמית

1 מבוא

מייל הקורס, המרצה, מדעי המחשב

מבנה הקורס:

- 2-3 שבועות ראשונים - לשכנע או להסביר מהי התרבות המרכזית של מדעי המחשב
- תוצאות אלמנטריות בתורת המספרים ואלגוריתמים, שקשורים אליהן
- קונגורואנציות RSA
- שאריות ריבועיות

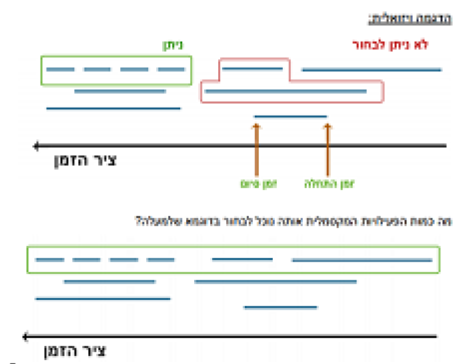
שיעור 1 - $17/10/18$

בעיית שיבוץ הפעילויות

ישנו חדר הרצאות יחיד, ויש אוסף של הרצאות, שלכל אחת זמן התחלה וזמן סיום. מטרה: למצוא את המספר המקס' של פעילויות שניתן לתִזמן בחדר כך שאלו לא יתנגשו

הערות:

- לא ניתן לשבור הרצאות (אין הפסקות)
- יום אחד



נסמן:

- ידוע לנו כמה פעילויות סה"כ - נסמנו ב n
- פעילות בודדת נסמן ב a_i , $1 \leq i \leq n$

דרך נוספת להצגת הבעיה, היא ע"י מערכים (מחשבים):

מערך לדוגמא:

נכניס לכאן את זמן ההתחלה של כל פעילות (s_i)

i=	1	2	3	4	5	6	7	8	9	10
	2.1	3	4.1 s_3	10	2.5	201	...	...	...	....

נכניס לכאן את זמן הסיום של כל פעילות (f_i)

i=	1	2	3	4	5	6	7	8	9	10
	5.5	7	4.2 f_3	11	5	305	...	...	...	....

איך מנסחים את הבעיה בצורה פורמלית:

- יהי $n \geq 1$ מספר שלם (טיבעי)
- ותהי $A := \{a_1, a_2, ..., a_n\}$ קבוצה של n פעיליות, כאשר לפעילות a_i , יש זמן התחלה s_i- , וזמן סיום - f_i.

1.0.1 הגדרה: קבוצה הינה אוסף <u>לא סדור</u> של איברים שונים.

קבוצות המספרים:

- $\mathbb{N}$- הטבעיים: $0, 1, 2, ...$
- $\mathbb{Z}$ - השלמים $... - 2, -1, 0, 1, 2....$
- $\mathbb{Q}$ - הרציונלים - מספרים הניתנים להצגה כמנה של שני שלמים - $\frac{1}{2}, \frac{3}{17}, ...$
- $\mathbb{R}$- הממשיים $\sqrt{2}, \pi, ...$
- $\mathbb{C}$ - המרוכבים

אינטרוולים - לדוג'$[3.5, 4]$

- קטעים פתוחים
- קטעים סגורים
- מעורבב - לדוגמה פתוח מצד וסגור מצד שני.

1.0.2 הגדרה: תהי Aקבוצה. כדי לומר שאיבר a שייך ל A נסמן $a \in A$

1.0.3 הגדרה: תהנה A ו- B זוג קבוצות ונגדיר $A \cap B := \{x : \ x \in A \ \wedge x \in B\}$

1.0.4 הגדרה: נסמן ב $\emptyset$ את הקבוצה הריקה.

1.0.5 הגדרה: $A \cap B = \emptyset$ המקיימות תנאי זה, יקראו קבוצות זרות

חזרה לבעיית הפעיליות - נזכר כי הגדרנו:

- יהי $n \geq 1$ מספר שלם (טיבעי)
- ותהי $A := \{a_1, a_2, ..., a_n\}$ קבוצה של n פעיליות, כאשר לפעילות a_i , יש זמן התחלה s_i- , וזמן סיום - f_i.
- יש למצוא תת קבוצה $S \subseteq A$ כך שזו מקיית שני תנאים:

1. (חוקיות) כל זוג פעיליות $a, b \in S$ מקיים $a \cap b = \emptyset$
2. (אופטימלית) מבין כל תתי הקבוצות של A המקימות את 1 ל s , יש את הגודל הכי גדול.

1.0.6 הגדרה: תהיה A ו B זוג קבוצות , נאמר ש B מוכלת ב A' ובכך מהווה תת־קבוצה של A. וכל $b \in B$ מקיים $b \in A$ או במתמטית: $\forall b \in B \, : \, b \in A$.

1.0.7 הגדרה: עבור קבוצה סופית A נסמן ב $|A|$ את כמות האיברים ב A.

<u>האלגוריתם:</u>

נסביר במילים: בכל שלב נבחר פיעליות שנחתכת עם הכי פחות פעיליות נשים אותה ב S ונסיר את כל מי שנחתך עימה. וכך נמשיך.... עד שלא יוותרו פעיליות.

הרציונל חמדני.

בהתחלה $S = \emptyset$ $A := \{a_1, a_2, a_3\}$

שלב 1: נבחר $S = \{a_3\}$ ע"פ הרעיון לעיל$A = \{a_1\}$

שלב 2: נצרף $S = \{a_3, a_1\}$ ו ־ $A = \emptyset$

להלן תיאור ב סאודו־קוד:

1. קלט $A : \{a_1, ..., a_k\}$
2. $s = \emptyset$
3. $while(A \neq \emptyset)$
4. a =: פעולות ב A שנחתכות עם הכי פחות פעיליות אחרות $S = S \cup \{a_i\}$
5. $A := A \backslash \{b \in A \; b \cap a \neq \emptyset\}$
6. חזרה ל $while$ (3)

1.0.8 הגדרה: תהינה A ו B זוג קבוצות נגדיר $A \cup B := \{x \, : x \in A \; or \; x \in B\}$ **ונאמר A איחוד B**

1.0.9 הגדרה: תהינה זוג קבוצות $A \backslash B := \{x \; : \; x \in A \, and \; x \notin B\}$

על מנת להוכיח שהאלגוריתם לעיל נכון יש להוכיח:

1. הקבוצה Sשמוחזרת ממנו חוקית
2. הקבוצה Sשמוחזרת ממנו בסוף להיותה חקוית הינה אופטמלית

<u>טענה: הקבוצה Sשמוחזרת חוקית</u>

מהאבחנה שהאלג, חמדן ולעולם לא מתחרט על בחירותינו נשים לב שמספיק להוכיח ש:

<u>טענה: לאורך כל האלגוריתם S חוקי</u>

<u>טענה: לכל $i \in \mathbb{N}$, בתחילת האיטראציה ה ־ i של לולאות ה $while$ הקבוצה s שנבנתה עד לזמן זה הינה קבוצה חוקית.</u>

.

*** חסר שיעור שבוע 2 ***

שיעור 3 ־ 31/10/2018

המטרה: אני רוצה להראות לכם שיטת ההצפנה בקריפטוגורפיה שנקראת RSA ־ זה לא סיפור קצר, היות וזה בפרט קשור לפקטוריצזיה

אינדוקציה

במסגרת ההוכחות שראינו עד כה השתמשו באינדוקציה, הגיע הזמן להגדיר זאת באופן מדויק.

נחזור לבעיית הפעילויות ־ המשך הסברים על אינדוקציה.

הפרכה תעשה ע"י דוגמה נגדית־מינימלית, העומדת על 'עיקרון הסדר הטוב': $\{x \in \mathbb{R} x > 0\}$ אני אומר לא, בעצם אני לא ב $\mathbb{R}$ אני ב $\mathbb{N}$ ואז $\{x \in \mathbb{N} :\ x < 0\}$.

<u>**אקסיומה:**</u> **עיקרון סדר הטוב** (WOP) **:**

בכל $s \subseteq N$ כך ש $s \neq \emptyset$ יש איבר מינימלי.
עקרון ראשון לאינדוקציה סופית:

משפט (אינדוקציה חלשה):

תהי $s \in \mathbb{N}$, $s \neq \emptyset$ אם זו מקיימת:

1. $1 \in s$ וגם:
2. אם $k \in s$ אזי $k+1 \in s$

אזי $s \in \mathbb{N}$.
<u>הוכחה:</u>

- תהי $s \in \mathbb{N}$ ו $s \neq \emptyset$ כך שזו מקיימת את התנאים לעיל. ונניח בשלילה כי $s \neq \mathbb{N}$ ונביט בקבוצה $T := \mathbb{N} \backslash s$.
- לפי wop היות ו $T \neq \emptyset$ נובע שיש ב T איבר מינימלי ויהיה זה a היות ו s מקיימת את תנאי 1 אז $a > 1$
- ואם כך המספר $a - 1 \in \mathbb{N}$.
- מהמינימליות של a ב T נובע ש $a - 1 \notin T$.
- לכן $a - 1 \in s$. היות ו $a \in s$, וזו סתירה.

$\square$

משפט: אינדוקציה חלשה ־ ניסוח אלטרנטיבי:

תהי $s(n)$. טענה מתמטית שתלויה ב $n \in \mathbb{N}$:
אם טענה זו מקיימת:

1. $s(1)$ נכונה, וגם
2. אם $s(k)$ נכונה אזי $s(k+1)$ נכונה.

אזי $s(n)$ נכונה.

בדיחות

<u>בדיחה 1</u>: כל המספרים הטבעים קטנים.
הוכחה באינדוקציה (חלשה) על גודל המספר.

1. 1 בוודאי קטן.
2. אם n קטן אז $n+1$ גם קטן כי רק הוספתי 1 .

הבעיה: קטן מ־??

<u>בדיחה 2</u>: כל החתולים בעולם באותו צבע.

הוכחה: באינדוקציה על כמות החתולים.

עבור חתול 1 , הטענה נכונה.

נניח שהטענה נכונה על קבוצות בגודל n ונשקול קבוצות בגודל $n+1$.

הבעיה: לא נכון בעבור $n=2$.

<u>המסר</u> ־ הוכחות אלו מאוד עדינות.

משפט: אינדוקציה חזקה ־ עיקרון שני לאינדוקציה סופית.

תהי $S\subseteq\mathbb{N}$, $S\neq\emptyset$, אם זו מקיימת:

1. $1\in S$
2. אם $\{1,2,3,......,n\}$ אז $n+1\in S$

אזי $S=\mathbb{N}$.

<u>מי חזק ומי חלש:</u>

לנו יש ביד אינדוקציה חלשה. על מנת להוכיח את משפט אינדוקציה חזקה. נותנים לי קבוצה S שמקיימת את 1,2 אז בפרט מקיימת את תנאי האינדוקציה החלשה ואז יש לי ש $s\in\mathbb{N}$, כנדרש.

הערה: החלש והחזק מתייחס לתנאי ההתחלתי (איפה אני דורש יותר = חזק)

לסיכום, עד עכשיו ראינו ש: אקסיומת WOP $\Leftarrow$ אינדוקציה חלשה $\Leftarrow$ אינדוקציה חזקה (**<u>יש טעות בהוכחה. אלעד תיקן בשיעור 4</u>**)

נראה ש: אינדוקציה חזקה $\Leftarrow$ WOP

<u>הוכחה:</u>

- נניח בשלילה ש WOP לא מתקיים, וקיימת קבוצה $s\in\mathbb{N}$, $s\neq\emptyset$, ללא איבר מינמלי. נראה ש $T=\mathbb{N}\backslash s$ מקיימת את תנאי האינד' החזקה.
- היות ו־ 1 איבר מינימלי ב $\mathbb{N}$, ולפי הנחה בשלילה ל s אין איבר מינימלי נובע ש $1\notin s$
- אם כך $1\in T$ ולכן T מקיימת את תנאי 1 לאינדוקציה חזקה.
- נניח ש $\{1,2,...,n\}\subseteq T$, יש להראות שמכך נובע ש $n+1\in T$:
- נניח בשלילה ש $n+1\in s$ היות ו $1,2,...,n$ אף אחד מהם לא ב s.
- ההנחה ש: $n+1\in s$ אומרת ש $n+1$ מינימלי ב s , וזו סתירה.

□

2 תורת המספרים

נתחיל מעולם השלמים $\mathbb{Z}$.

2.0.1 הגדרה: אם aו b זוג שלמים שלמים נרשום $a|b$ לציין ש a מחלק את b . כלומר ישנו $k \in \mathbb{Z}$ כך ש $b = a \cdot k$.

לדוגמה $12,7$ מתקיים ש : $12 = 7 \cdot 1 + 5$

באופן כללי בעבור a ו b :

- אם $r = 0$ אזי $b|a$
- אם $r > 0$ אם $b \nmid a$ בודאות אתם רואים $r < b$

משפט החלוקה

יהיו a ו b שלמים גדולים מאפס.

אז קיימים זוג מספרים r ו q ייחודים כך ש $0 \le r \le b$ ומתקיים $a = qb + r$

הוכחה־ קיום:

- בהינתן a ו ־ b נגדיר: $S := \{a - b \cdot k : k \in \mathbb{Z}, a - bk \ge 0\}$ (קבוצת ההפרשים)
- ניתן לראות ש $S \ne \emptyset$, ־ ניקח k, b חיוביים , וככל שהkים גדולים יותר הקבוצה גדולה יותר...

  (אבל יתכן ש $0 \in S$ ואז לא נוכל לומר ש $s \subseteq \mathbb{N}$, אבל WOP נכון בעבור גם $\mathbb{Z}^+$, וזה מספיק לנו.)
- אם כן, בקבוצה S ישנו איבר מינימלי יהיה זה r (ע"פ WOP), כלומר קיים q כך ש: $r = a - qb$.

  נותר להראות ש: $0 \le r \le b$:
- מצד אחד, לפי הגדרת S , $0 \le r$.
- מצד שני, נניח בשלילה כי $r \ge b$ אז:

$$r \ge r - b = \underbrace{a - qb}_{=r} - b = \underbrace{a - b(q+1)}_{\in S} \ge 0$$

- בסתירה למינימליות של r .

יחידות q ו r:

נניח בשלילה שאינם יחידים ואז ניתן לרשום כי:

- $a = q_1 b + r_1 \ , \ 0 \le r_1 < b$
- $a = q_2 b + r_2 \ , \ 0 \le r_2 \le b$
- יתקיים ש (השוואת ה־ a) :

$$0 = b\,(q_1 - q_2) + (r_1 - r_2) \Rightarrow r_2 - r_1 = b\,(q_1 - q_2)$$

- נובע ש $b|\,(r_2 - r_1)$ ומכאן נובע ש: $-b < r_2 - r_1 < b$ (כי $r_2 - r_1$ הינו כפולה של b)$\Leftarrow$ $r_2 - r_1 = 0$ $\Leftarrow$ $r_2 = r_1$ בסתירה לכך שהם שונים.

$\square$

שיעור 4 - 7/11/18

תזכורת: בשבוע שעבר הצגנו שני משפטים: אינדוקציה חזקה וחלשה, והראנו את השקילות בין אקסיומת הסדר הטוב, לחלשה לחזקה. היום נראה שוב את הוכחת משפט החלוקה.

טעות משבוע שעבר: הראנו את שחזקה גוררת חלשה. נראה אם כן את המשפט מהתחלה.

משפט: אינדוקציה חזקה $\iff$ אינדוקציה חלשה

<u>כיוון ראשון: חלשה $\Leftarrow$ חזקה</u> - הוכחה:

תהי $s \subseteq \mathbb{N}$ שזו המקיימת את תנאי האינדקוציה החלשה יש להראות ש $s = \mathbb{N}$. כך שזו מקיימת $S.1$ ואת $S.2$

- הטענה ש $1 \in S$, נובעת באופן טריוויאלי, שכן $I.1$ ו $S.1$ זהים.
- עבור קיום של $S.2$ ניתן לראות שאם קבוצה מקיימת את $I.2$, אז זו מקיימת גם $S.2$

<u>כיוון שני: חזקה $\Leftarrow$ חלשה:</u>

נתונה קבוצה $S \subseteq \mathbb{N}$ כך שזו מקיימת את $S.1$ ו $S.2$ יש להראות ש $S = \mathbb{N}$

- נגדיר: $Q := \{n \in \mathbb{N} : \ k \in s \ \forall k < n\} \cup \{1\}$אם נראה ש $Q = \mathbb{N}$,אז סיימנו ו $s = \mathbb{N}$.

  נראה זאת: נניח ש $Q = \mathbb{N}$ ונוכיח ש $\mathbb{N} \subseteq \mathbb{S}$ יהי $n \in \mathbb{N}$.

  - לפי ההנחה $Q = \mathbb{N}$ ולכן $n \in \mathbb{Q}$.
  - אם כך לפי הגדרת Q:$S \subseteq \{1, 2, ..., n-1\}$
  - אז לפי $S.2$ אותה S מקיימת .נובע ש : $n \in S$
- נוכיח אם כן, ש $Q = \mathbb{N}$:

  נשתמש באינדוקציה חלשה כדי להוכיח זאת.

  - היות ו $1 \in \mathbb{Q}$ לפי לפי הגדרה $I.1$ מתקיים עבור Q .
  - נותר לוודא את $I.2$ עבור Q. כלומר יש להראות שאם n∈Q אזי $n+1 \in Q$.
  - אם $n \in Q$ אזי $\{1, 2, 3, ..., n-1\} \subseteq S$ לפי הגדרת Q .
  - לכן לפי $S.2$ $n \in S$ מה שאומר כי $\{1, 2, ..., n\} \subseteq S$
  - וכעת לפי הגדרת Q , $n+1 \in \mathbb{Q}$

משפט: יהי $a, b \in \mathbb{Z}$ **אז קיימים זוג מספרים** q **ו** r **יחודים כך ש:** $a = q \cdot b + r$ **וגם** $0 \leq r < b$

הוכחה: ישנן שתי טענות כאן, קיום ויחודיות.

<u>קיום:</u>

- נגדיר: $s = \{a - bk : \ k \in \mathbb{Z}, \ a - bk \geq 0\}$
- הקבוצה הינה קבוצה לא ריקה ב $\mathbb{Z}^+$ ולכן לפי WOP יש לה איבר מינימלי.
- יהיה זה r ונרשום $r \leq a - qb$ עבור q כלשהו ב $\mathbb{Z}$.
- קיום r מעיד על קיום q.
- מהגדרת sנבוע ש $r \geq 0$ נותר להראות ש $r < b$

- נניח בשלילה אם כך ש: $r \geq b$, כעת:

$$r \geq r-b=\underbrace{a-qb}_{=r}-b=\underbrace{a-b(q+1)}_{\in S}\geq 0$$

- כאשר הביטוי גדול כולו מאפס מההנחה ש $r \geq b$. שכן $a-(q+1)\,b>r-b\geq 0$
- וכעת אם כך $a=(q+1)\,b\in S$
- ובנוסף $a-(q+1)\,b<r$
- וזו סתירה ממינמליות של r ב S .

<u>יחודיות:</u>

ננניח בשלילה שאינם יחידים ואז ניתן לרשום כי:

- $a=q_1b+r_1$, $0\leq r_1<b$
- $a=q_2b+r_2$, $0\leq r_2\leq b$
- יתקיים ש (השוואת ה־ a) :

$$0=b\left(q_1-q_2\right)+\left(r_1-r_2\right)\Rightarrow r_2-r_1=b\left(q_1-q_2\right)$$

- נובע ש $b|\left(r_2-r_1\right)$ ומכאן נובע ש: $-b<r_2-r_1<b$ (כי r_2-r_1 הינו כפולה של b) $\Leftarrow 0=r_2-r_1\Leftarrow r_2=r_1$ בסתירה לכך שהם שונים.

$\square$

GCD

2.0.2 הגדרה: יהיו $a,b\in\mathbb{Z}$, $0<a,b$ המחלק המשותף הגדול ביותר של a ו b נקרא ה gcd של a ו־ b : $greatest-common-divisor$ **ונסמנו ב (a,b) וכמובן שניתן לרשום (b,a) .**

דוגמה:

$$(12,6)=6$$
$$(3,2)=1$$
$$(108203,108202)=1$$

מטרה שולית: RSA . בדרך שלנו לתכנן אלגוריתם: שבהינתן $a\geq b>0$ שלמים יחשב את (a,b)
עבור $n\in\mathbb{Z}^+$ הגדרתם $D(n)=\{b\in\mathbb{Z}:d|n\}$. ואז מצאתם $D(12)\cap D(6)$ ובחרתם max . אבל זה לא יעיל.

משפט $bezout$:

2.0.3 הגדרה: עבור $a,b\in\mathbb{Z}$ נגדיר את הקבוצה : $L(a,b):=\{ma+nb:\ m,n\in\mathbb{Z}\}$

המשפט: $(a,b)\in L(a,b)\cap\mathbb{Z}^+$ ובפרט איבר מינימלי שם.

הוכחה:

- הקבוצה $L(a,b)\cap\mathbb{Z}^+$ אינה ריקה, ולכן יהי $d\in L(a,b)\cap\mathbb{Z}^+$

- $d = ma + nb$ ומינימלי ב $L(a,b)\cap\mathbb{Z}^+$ מ wop .
- נרצה להראות ש $d=(a,b)$, כלומר נראה ש:

1. $d|a$
2. $d|b$

1,2 - טוענים שd הוא פתרון אפשרי.

3. $d = Max\left\{D(a)\cap D(b)\right\}$ - כלומר d הוא פתרון אופטימלי

נראה תחילה ש $d|a$ הטיעון ש $d|b$ סימטרי:

- לפי משפט החלוקה ניתן לרשום $a = qd + r$ כך ש $0\le r<b$
- אם $r=0$ סיימנו שכן מתקיים $d|a$ לפי הגדרה.
- נניח אם כן ש $r>0$, ויתקיים

$$0 < r = a - dq = a - q\left(ma+nb\right) = \underbrace{(1-qm)a + \left(-qn\right)b}_{\in L(a,b)\cap\mathbb{Z}^+}$$

- המספר $(1-qm)a + \left(-qn\right)b \in (a,b)$, היות וזה שווה ל r ו $0<r$ נקבל ש:

$$(1-qm)a + \left(-qn\right)b \in L(a,b)\cap\mathbb{Z}^+$$

- השיוון של מספר ה ל r מעיד ש $(1-qm)a + \left(-qn\right)b < d$
- לכן $r<d$ וזו סתירה למינימליות של d ב $L(a,b)\cap\mathbb{Z}^+$

הראנו את 1, ו2 סימטרי ל1 , על כן נותר להראות את 3 (אופטימליות) $d = Max\left\{D(a)\cap D(b)\right\}$, מספיק להראות שמתקיים:

$$c|d \qquad \forall c\in D(a)\cap D(b)$$
$$\tfrac{d}{c} = \tfrac{ma+nb}{c} = m\underbrace{\frac{a}{c}}_{\in\mathbb{Z}} + n\underbrace{\frac{b}{c}}_{\in\mathbb{Z}}$$

שיעור 5 - 14/11/18

חזרה קצרה:

משפט $(bezout)$: אם $a,b\in\mathbb{Z}$ אז $(a,b)\in L(a,b)\cap\mathbb{N}$. ובפרט מינימלי בקבוצה זו

הגדרה (אלטרנטיבית ל gcd):

יהיו a ו b שלמים, נסמן ב (a,b) מספר שמקיים:

1. אם $(a,b)\,|a$ וגם $(a,b)\,|b$
2. לכל c שלם כך ש $c|a$ וגם $c|b$ מתקיים $c|(a,b)$

2.0.4 **הגדרה: שני שלמים a ו b יקראו זרים אם $(a,b)=1$**

איך הגדרת זרים ו $bezout$ קשורים?

אם $(a,b)=1$ עבור $a,b\in\mathbb{Z}$ אז לפי $bezout$יתקיים:

$$\exists m,n\in\mathbb{Z}:\ 1=ma+nb$$

לדוגמה:

$$1=7\cdot3+(-4)\cdot5\in L(3,5)\cap\mathbb{N}$$
$$(3,5)=1$$

משפט: אם $a|c$ ו $b|c$ וגם (a,b) אזי $ab|c$

הוכחה:

$$c\overset{1}{=}c\cdot1\overset{2}{=}c(am+nb)\overset{1}{=}cam+cbn$$

1. לא עשינו דבר . 2. משפט $bezout$

- היות ו $a|c$ קיים $k\in\mathbb{Z}$ מכך ש $c=ka$
- היום ו $b|c$ קיים $l\in\mathbb{Z}$ כך ש $c=lb$
- כעת:

$$c=labm+kabn=ab(lm+kn)$$

ובסה"כ $ab|c$, כנדרש.

$\square$

באופן כללי הטענה: אם $a|bc$ אזי $a|b$ או $a|c$ אינה נכונה, דוגמה

$$4|6\cdot2\qquad 4\nmid2\qquad 4\nmid6$$

משפט: אם $a|bc$ ו $(a,b)=1$ אזי $a|c$:

הוכחה:

יהיו $x,y\in\mathbb{Z}$

$$c\overset{1}{=}c\cdot1\overset{2}{=}c(ax+by)\overset{1}{=}c\boldsymbol{a}x+\underbrace{cby}_{a|bc}$$

ובסה"כ $a|c$, כנדרש.

$\square$

משפט: כל שלם אם $n > 1$ ניתן להביע אותו באופן ייחודי כמכפלה של ראשוניים כך ש:

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot, ..., p_n^{a_k}$$

כך ש:

$$p_1 < p_2 < ..... < p_n$$

ובנוסף $a_i \geq 1$ לכל $i \in [k]$

דוגמה

$$a = 2^5 \cdot 3^{17} \cdot 7^{18}$$
$$b = 2^4 \cdot 5 \cdot 7^{21}$$
$$(a,b) = 2^4 \cdot 7^{18}$$
$$= 2^{min(5,4)} 3^{min(0,17).....}$$

משפט: לכל $n > 1$ שלם קיים מחלק ראשוני

הוכחה:

- נניח בשלילה שקיים $n > 1$ שאין לו מחלק ראשוני.
- לפי WOP ניתן לבחור את n שכזה **מינמלי** . וגם כך ש n איננו ראשוני שכן אז ההנחה נופלת באופן מיידי.
- מכך ש n אינו ראשוני , ניתן להניח ש n פריק, ומכאן שקיימים $a, b \in \mathbb{Z}$ כך ש $2 \leq a, b < n$ כך ש: $n = ab$
- היות ו $2 \leq a < n$ זה לא מהווה דוגמה נגדית למשפט. ולכן קיים p ראשוני כך ש $p|a$ נקבל ש: $a|n$ וגם $p|a$ אזי $p|n$

משפט : לכל $n > 1$ שלם ופריק יש מחלק ראשוני $\leq \sqrt{n}$

- יהי $n = ab$ כך $2 \leq a, b < n$
- ניתן להניח שלפחות אחד מ a ו b הינו $\leq \sqrt{n}$ שכן אחרת $ab > n$
- נניח שזהו a כלומר $a \leq \sqrt{n}$.
- לפי משפט קודם ל a יש מחלק ראשוני

$\square$

משפט: אם p ראשוני ובנוסף $p|ab$ אזי $p|a$ או $p|b$

נזכר שהוכחנו שאם $a|bc$ ו $(a,b) = 1$ אזי $a|c$

הוכחה:

- אם $p|a$ סיימנו, ולכן נניח שלא . כלומר $p \nmid a$ ומכאן ש $(p,a) = 1$
- וכעת ממשפט קודם: $p|b$

משפט: יהי p ראשוני ויהיו $a_1, ..., a_k$ שלמים כך ש $p|a_1 \cdot .... \cdot a_n$ אז קיים $j \in [n]$ כך ש $p|a_j$

למשל: $3 \cdot 2 \cdot 2 = 2 \cdot 6|4$ או $3|12 = 2 \cdot 3 \cdot 2$

הוכחה:

<u>בסיס:</u>

עבור $n = 1$ הטענה טריוויאלית ועבור $n = 2$ אפילו הוכחנו במשפט קודם.

<u>צעד:</u> נניח כי הטענה נכונה ל n ונכיח בעבור $n + 1$

נתון כי $p|a_1 \cdot ...... \cdot a_n \cdot a_{n+1}$. <u>צ"ל</u> יש להראות שקיים $j \in [n + 1]$ כך $p \cdot a_j$.

- אם $p|a_1 \cdot ..... \cdot a_n$ אז מהנחת האינדוקציה סיימנו.
- על כן נניח כי $\cancel{p|a_1} \cdot .... \cdot a_n$ ולכן $(p, a_1 \cdot .... \cdot a_n) = 1$
- וממשפט קודם: $p|a_{n+1}$

$\square$

משפט: כל $1 < n$ ניתן להביעו כמכפלה של ראשוניים באופן ייחוד עד כדי סדר

הוכחה - צריך להראות קיום וייחודיות:

<u>קיום:</u>

- נניח בשלילה שקיים $1 < n$ שאין לו כזה פירוק.
- לפי WOP ניתן לבחור n שכזה מינמלי מבין כל הדוגמאות נגדיות
- אם כך n איננו ראשוני שכן אחרת לא יהווה דוגמה נגדית.
- כלומר

$$n = ab$$
$$2 \leq a, n < n$$

- היות ו$2 \leq a, b < n$ אלו לא מהווים דוגמה נגדית .
- ולכן לכל אחד מהם יש פירוק כפי שראינו ולכן גם ל n , וזו סתירה.

<u>יחיד:</u>

נזכר במשפט: יהי p ראשוניים ויהיו $q_1, ..., q_n$ ראשונים כך ש $p|q_1 \cdot ... \cdot q_n$ אז קיים $j \in [n]$ כך ש: $p = q_j$

- נניח כי קיים $1 < n$ כך ש: $p_1 \cdot ...... \cdot p_m = n = q_1 \cdot ..... \cdot q_n$ כך שייצוגים שונים.
- נוכל להניח שאין כפיליות בין הגורמים של $p_1, ..., p_m$, $q_1, ..., q_{n-1}$, שכן אם יש נוכל לצמצם.
- אם כך נוכל לרשום ש: $q_1 \cdot ..... \cdot q_n = p_1 \left(p_2 \cdot ...... \cdot p_m\right)$
- ולהסיק ש: $p_1|q_1 \cdot ..... \cdot q_n$ אז לפי המשפט קיים $j \in [n]$ כך ש $p_i = q_j$ בסתירה לכך שאין גורמים משותפים בין הייצוגים.

תרגיל: נתונה המשוואה $3x+6y=18$, האם משוואה זו פתירה ב $\mathbb{Z}$?

כלומר, האם קיימים $x_0, y_0 \in \mathbb{Z}$ כך שאם נציב $x = x_0$ ו $y = y_0$ המשוואה תהיה נכונה?

אצלנו:

$$3 \cdot 1 + 6 \cdot 1 = 18$$
$$3(-6) + 6 \cdot 6 = 18$$
$$3 \cdot 10 + 6 \cdot (-2) = 18$$

דוגמה נוספת: $\underbrace{17}_{odd} = \underbrace{2x+10y}_{even}$ ולכן אינו פתיר מעל $\mathbb{Z}$

שאלה: בהנתן $a, b, c \in \mathbb{Z}$ איך נדע שאם $ax + by = c$ פתירה מעל $\mathbb{Z}$?

משפט: יהיו $a, b, c \in \mathbb{Z}$ **,** $ax + by = c$ **פתירה** $\iff gcd(a,b)|c$

הוכחה - נראה גרירה דו-כיוונית:

כיוון ראשון: $ax + by = c$ פתירה $\Leftarrow gcd(a,b)|c$

- נניח כי x_0, y_0 מהווים פתרון למשוואה דהיינו $ax_0 + by_0 = c$
- לכן קיימים $k, l \in \mathbb{Z}$ כך ש $\underbrace{(a,b)k}_{a} x_0 + \underbrace{(a,b)l}_{b} y_0 = c$
- כעת אם נחלק ב (a,b) נקבל ש: $kx_0 + ly_0 = \frac{c}{(a,b)}$
- צד שמאל של המשוואה הם כולם מספרים שלמים, ובפרט $\frac{c}{(a,b)}$ מספר שלם, כנדרש.

כיוון שני: $ax + by = c$ פתירה $\Rightarrow gcd(a,b)|c$:

- נניח כי $(a,b)|c$ אז ישנו $l \in \mathbb{Z}$ כך ש :

$$c = (a,b))\, l \overset{\text{bezout}}{=} (am + bn)l = aml + bnl$$

- על כן, אם נגדיר $ml = x_0$ ואת $nl = y_0$ נקבל את הדרוש.

$\square$

אלגוריתם אקולידס לחישוב gcd:

קלט: $a \geq b \geq 0$

פלט: $gcd(a,b)$

```
Euclid(a,b):
    if b=0
        return a
    else
        return Euclid(b,a mod b)
```

טענה: לכל $a \geq b \geq 0$ **שלמים** $Euclid(a,b) = gcd(a,b)$ **(הרצת האלגוריתם תחזיר את ה**gcd**)**

דוגמה מספרית: $a = 72, b = 30,$ $\Leftarrow$ $gcd(72,30) = 6$

$$\begin{array}{llllll}
Euclid(72,30) & & & & & \\
\quad\hookrightarrow & [72 = 2\cdot 30 + 12] & & & & \\
 & Euclid(30,12) & & & & \\
 & \quad\hookrightarrow & [30 = 2\cdot 12 + 6] & & & \\
 & & Euclid(12,6) & & & \\
 & & \quad\hookrightarrow & [12 = 2\cdot 6 + 0] & & \\
 & & & Euclid(6,0) & & \\
 & & & \text{return } 6 & &
\end{array}$$

מדוע האלגוריתם עוצר?

נתבונן בסדרה הנוצרת מערכי הפרמטר b לאורך הרצת האלגריתם:

$$b, a \mod b,\ b \mod (a \mod b),\ (a \mod b) \mod (b \mod (a \mod b)),\ ....$$

נגדיר $x_1 = b$, $x_1 = a \mod b$, $x_{i+1} = x_{i-1} \mod x_i$

טענה: לכל $2 \leq i \in \mathbb{Z}$ **מתקיים** $x_i \leq b - (i-1)$

<u>אם טענה זו נכונה:</u> אז קיים $2 \leq i$ כך ש $x_i \leq 0$ בפרט אם ניקח $i = b+1$ ואז לכל i (גם לx_1 כי $b \geq 0$ בהתחלה) . בפרט יתקיים בעבור:

$$x_{b+1} \leq b - (b+1-1) = 0$$

<u>מצד שני</u> כל ה x_iים "באים" ממשפט החלוקה, ולכן לכל x_i, $x_i \geq 0$, ובפרט ל x_{b+1},

<u>בסה"כ:</u>

$$0 \leq x_{b+1} \leq 0 \text{ ולכן } x_{b+1} = 0$$

<u>הוכחה ־ באינדוקציה על i :</u>

<u>בסיס: </u>עבור $i = 0$ ממשפט החלוקה $x_2 = a \mod b \leq b - 1 = b - (2-1)$

נניח שהטענה נכונה בעבור i ונוכיח ל $i+1$:

$$x_{i+1} \overset{1}{=} x_{i-1} mod\ x_i \overset{2}{\leq} x_i - 1 \overset{3}{\leq} b - (i-1) - 1 = b - i = b - ((i+1)-1)$$

1. מהגדרת הסדרה. 2. ממשפט החלוקה . 3. הנחת האינדוקציה

$\square$

ראינו שהאלגוריתם עוצר לכל $a \geq b \geq 0$, מה הוא מחזיר?

נרצה להוכיח $Euclid(a,b) = gcd(a,b)$

<u>הרעיון:</u>

$$(a,b) \to (b, a \mod b) \to (a \mod b, b \mod (a \mod b) \to (a,0) = a$$

משפט: יהיו a,b,c **אז** $gcd(a,b)=gcd(a+bc,b)$

הוכחה:

נסמן ב D את קבוצת המחלקים, אז מסמספיק להראות ש:

$$D(a)\cap D(b)=D(a+cb)\cap D(b)$$

כיוון ראשון: $D(a)\cap D(b)\subseteq D(a+cb)\cap D(b)$

נזכר במשפט: אם $c|a$ וגם $c|b$ אז $c|a\pm b$

יהי $e\in D(a)\cap D(b)$ לפי הגדרה $e\in D(b)$ היות ו $e|b$ וגם $e|a$ אז נוכל לומר ש $e|a+b$ ובפרט $e|a+bc$ כנדרש.

כיוון שני: $D(a+cb)\cap D(b)\subseteq D(a)\cap D(b)$

יהי $f\in D(a+cb)\cap D(b)$ היות ו $f|b$ נותר להראות ש $f|(a)$,

מתקיים ש: $a=(a+bc)-bc$ ונתון כי $f|b$ ו$f|a+bc$ אז גם $f|a$, כנדרש.

.

משפט: יהי $a\geq b\geq 1$ **אז** $gcd(a,b)=(b,a \mod b)$

מתקיים ש: $a=\left\lfloor \frac{a}{b}\right\rfloor b+a \mod b$

כלומר $a \mod b=a+\left(-\left\lfloor \frac{a}{b}\right\rfloor b\right)$

ואז ממשפט קודם:

$$gcd\left(a, \mod b\right)=gcd\left(a,b\right)=gcd\left(a+\left(-\left\lfloor \frac{a}{b}\right\rfloor b\right),b\right)$$

מספרים ראשוניים:

מסקנה מהמשפט היסודי: המספרים הראשוניים הינם 'אטומים' שבונים את כל $\mathbb{Z}$

$$n=p^{a_1}p_2^{a_2}\cdot ...p_k^{a_k}$$

$Euclid$ שאל: כמה אטומים יש בעולם שלנו? כמה ראשוניים יש בעולם?

משפט: יש ∞ **ראשוניים בעולם**

הוכחה: נניח בשלילה שישנו מספר סופי של ראשוניים בעולם. ויהיו $p_1,p_2,...,p_n$ קבוצות כל הראשוניים בעולם.

- נגדיר : $Q:=p_1\cdot p_2\cdot ...\cdot p_n+1$
- היות ו $Q>p_n$ אז q פריק ולכן קיים לו מחלק ראשוני q , לפי משפט משיעור שעבר אם $q\in\{p_1,...,p_n\}$ אז ישנו $q=p_j$ כך ש $q|p_1\cdot p_2\cdot ...p_n$
- היות ו $q|Q$ לפי הגדרה נובע ש $q|Q-p_1p_2\cdot ...\cdot p_n$ כלומר $q|1$ אבל q ראשוני
- ולכן $Q\leq q$, וזו סתירה

שיעור 7 - 28/11/18

איפה אנחנו עומדים?

הראינו את המשפט היסודי של הארתמיטקה $n = p_1^{a_1} p_2^{a_2}, ..., p_k^{a_k}$ $a_i \geq 1$ לכל $i \in [k]$, $n \in \mathbb{Z}$,

ואת המשפט: (ניסוח 2) יש ∞ ראשוניים בעולם . והיום נתחיל מלנסח אותו אחרת.

מדוע?

<u>מוטוביציה:</u>

אנחנו פוגשים סדרות באופן טבעי על ידי ניתוח לולאות: חשבוניות, פיבונאצ'י ועוד. ועולה השאלה האם יש סדרה:

P_n =: המספר הראשוני ה n .

<u>ניסוח 2:</u> לכל $n \geq 1$ מתקיים: $p_{n+1} \leq p_1, p_2, ..., p_n + 1$

הוכחה בציור.

משפט: לכל $n \geq$ **:** $p_n \leq 2^{2^n}$

הוכחה:

<u>בסיס:</u> נתבנון רגע בסדרת החזקות: $\begin{matrix} 2^{2^0} = 2 \\ 2^{2^1} = 4 \\ 2^{2^2} = 16 \\ \vdots \end{matrix}$ ומצד שני $\begin{matrix} p_1 = 2^2 \leq 2^2 \\ p_2 = 3 \leq 16 \end{matrix}$

<u>צעד:</u> נניח שהטענה נכונה לכל $k \leq n$ ונשקול P_{n+1}, כלומר <u>נרצה להוכיח ש</u> $p_{n+1} \leq 2^{2^{n+1}}$

1. ממשפט $Euclid$ - ניסוח 2 - נובע:

$$P_{n+1} \overset{1}{=} p_1 p_2 \cdot .... \cdot p_{n+1} + 1 \overset{2}{\leq} 2^{2^1} 2^{2^2} ....2^{2^n} + 1 \overset{3}{=} 2^{\sum_{i=1}^{n} 2^i} + 1 \overset{4}{\leq} 2^{2^{n+1}-1} + 1 \overset{5}{\leq} 2 \cdot 2^{2^{n+1}-1} = 2^{2^{n+1}}$$

2. הנחת האינדוקציה. 3. חוקי חזקות. 4. מהוכחה שראינו בתרגול נובע ש: $\sum_{i=1}^{k} 2^k = 2^{k+1} - 1$ 5. קל להראות באינדוקציה.

$\square$

האם אפשר יותר טוב?

$$p_1 = 2 \leq 2^1$$
$$p_2 = 3 \leq 2^2$$
$$p_3 = 2 \leq 2^3$$

משפט $bertrand$ **: לכל** $n \geq 2$ **ישנו ראשוני (לפחות אחד) באינטרוול הפתוח** $(n, 2n)$

נדגים:

$$n = 1 \text{ not included}$$
$$n = 2 \Rightarrow 3 \in (2, 4)$$
$$n = 3 \Rightarrow 5 \in (5, 6)$$

לא נוכיח, אבל תכף נשתמש...

משפט: לכל $n \geq 2$ **:** $p_n < 2^n$

הוכחה:

באינדוקציה על n :

בסיס: כפי שראינו: $p_1 = 2 \leq 2^1$, $p_2 = 3 \leq 2^2$, $p_3 = 2 \leq 2^3$

צעד: נניח כי $p_n < 2^n$ ונוכיח כי $p_{n+1} < 2^{n+1}$:

- לפי $bertrand$ האינטרוול $\left(2^n, 2^{n+1}\right)$ מכיל ראשוני q , ומהנחת האינדוקציה:

$$p_n < 2^n < q < 2^{n+1}$$

- נובע ש $q \leq p_{n+1}$ שכן אין ראשוניים בין p_n ל p_{n+1}
- בפרט יתקיים ש: $p_{n+1} \leq q < 2^{n+1}$

$\square$

משפט $Dirichlet$: $gcd(a,b) = 1$ אז בסדרה $an + b$ יש ∞ ראשוניים.

משפט: יש אינסוף ראשוניים מהצורה $4n + 3$

<u>ניסיון כושל:</u>

- נניח שיש מספר סופי של ראשוניים מהצורה $4n + 3$, יהיו אלה $q_1 q_2, , ..., q_n$ כלומר $3, 7, 11, ...$.
- נגדיר $Q := 4\left(q_1, ..., q_n\right) + 3$
- היות ו Q אי־זוגי, 2 איננו פקטור של Q
- היות ו Q מהצורה $4n + 3$ איננו ראשוני $q_n < Q$
- יש ל Q מחלק ראשוני q (q חייב להיות אי־זוגי)
  - נניח בשלילה שq הוא מהצורה $4n + 1$
  - נברר אם כן, כיצד נראה מספר שכל הפקטורים שלו מהצורה $4n + 1$?

$$\left(4n+1\right)\left(4m+1\right) = .. = 4\left(4mn + n + m\right) + 1$$

  - כלומר באינדוקציה כל מספר מהצורה $4n + 1$ ישאר מהצורה $4n + 1$,
- ולכן q מהצורה $4n + 3$
- נניח ש $q \in \{q_1, q_2, ..., q_n\}$ אז $3 \leq q | Q - 4\left(\overset{=3}{q_1} q_2, ..., q_n\right) - 3$

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

הוכחה: יש להראות הכלה דו־כיוונית

- כיוון ראשון $\{4n-1 : n\in\mathbb{Z}\} \subseteq \{4n+3 : n\in\mathbb{Z}\}$
  - יהיה $z\in\{4n-1 : n\in\mathbb{Z}\}$ צ"ל $z\in\{4n+3 : n\in\mathbb{Z}\}$
    - מכך ש $z\in\{4n-1 : n\in\mathbb{Z}\}$ קיים $n'\in\mathbb{Z}$ כך ש:
$$z = 4n'-1 = 4n'-4+4-1 = 4(n'-1)+4-1$$
    - על כן אם נסמן $m' = n'-1$ נקבל:
$$4(n'-1)+4-1 = 4m'+3$$
    - לכן $z\in\{4n+3 : n\in\mathbb{Z}\}$
- כיוון שני $\{4n-1 : n\in\mathbb{Z}\} \subseteq \{4n+3 : n\in\mathbb{Z}\}$:
  - סימטרי

נסכם:

משפט: יש ∞ ראשוניים מהצורה $4n+3$

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

משפט 2 : מספר שהינו מכפלה של מספרים מהצורה $4n+1$ הינו $4n+1$ בעצמו

הוכחה:

- נניח בשלילה שישנו מספר סופי של ראשוניים מהצורה $4n+3$, יהיהו q,q_1,q_n ראשוניים אלו
- נגדיר $Q := 4q_1q_2,...,q_n-1$ ולפי משפט 1 , Q הינו מהצורה $4n+3$
- היות ו Q אי־זוגי ולפי משפט 2 יש ל Q מחלק ראשוני מהצורה $4n+3$, נסמנו ב q
- נניח בשלילה ש: $q\in\{q_1,q_2,....,q_n\}$
- אם כך (מאוקלידס) $3\le q|Q-4q_1,....q_n = -1$ וזו סתירה.

3 קונגרואנציות

3.0.1 הגדרה: יהי $m\in\mathbb{Z}^+$ והיו $a,b\in\mathbb{Z}$, נאמר ש a קונוגורואנטי ל b מודולו m ונרשום $a\equiv b\ (\mod n)$ או $a\equiv b(m)$

דוגמה:

1. $2|6-4 \Leftarrow 4\equiv 6(2)$
2. $2|1-(-1) = 2\equiv -(1)2$
3. $n|(n-1)-(-1) \to n-1\equiv -1(n)$
4. $n|(n-i)-(-i) \to n-i\equiv -i(n)$

בדרך להבנת ההגדרה:

משפט:

$$a \equiv b(\mod m) \iff \exists k \in \mathbb{Z}\ a = bkm$$

הוכחה:

כיוון ראשון: $a \equiv b(\mod m) \Rightarrow \exists k \in \mathbb{Z}\ a = bkm$:

נניח ש $m|a-b$ אז קיים $k \in Z$ כך ש $a-b=km$ ולכן $a=bkm$, כנדרש:

כיוון שני: $a \equiv b(\mod m) \Leftarrow \exists k \in \mathbb{Z}\ a+bkm$:

ולכן $a-b \equiv mk$ ולכן $m|a--b$ ולכן $a \equiv b(m)$

$\square$

משפט:

$$\text{ל } a \text{ ול } b \text{ אותה שארית אחרי חלוקה ב } m \iff a=b(m)$$

כלומר:

$$a=b(m) \iff a=km+\boldsymbol{r}\ ,b=lm+\boldsymbol{r}$$

בלוגיקה היינו מנסחים:

$$R_m := \{(a,b) \in \mathbb{Z} \times \mathbb{Z} : a \equiv b(m)\}$$

<u>הוכחה:</u>

$a=b(m)\boldsymbol{:} \Rightarrow a=km+\boldsymbol{r}\ ,b=lm+\boldsymbol{r}$

- נניח ש $a \equiv b(m)$ ממשפט קודם קיים $k \in \mathbb{Z}$ כך ש: $a=b+km$
- ע"פ משפט החלוקה עבור b ו m ישנו l כך ש: $b=lm+r$
- ואז $a=(l+k)m+r$

$a=b(m)\boldsymbol{:} \Leftarrow a=km+\boldsymbol{r}\ ,b=lm+\boldsymbol{r}$

- נניח ש $a=km+\boldsymbol{r}\ ,b=lm+\boldsymbol{r}$ יש להראות $m|a-b$
- נשים לב ש: $a-b=(k-l)m$ ולכן $m|a-b$

שיעור 8 - 05/12/18

תזכורת משיעור שעבר:

- הגדרה: יהי $m \in \mathbb{Z}^+$ והיו $a,b \in \mathbb{Z}$, נאמר ש a קונוגוראנטי ל b מודולו m ונרשום $a \equiv b\,(\mod n)$ או $a \equiv b(m)$
- משפט: $a \equiv b(\mod m) \iff \exists k \in \mathbb{Z}\ a+bkm$
- משפט: ל a ול b אותה שארית אחרי חלוקה ב $m \iff a=b(m)$

3.0.2 הגדרה: יחס דו־מקומי שהינו רפלקסיבי, סימטרי, טרנזיטיבי נקרא יחס שקילות

- רפלקסיביות: לכל $a \in \mathbb{Z}$: $a, b \in R_m$
- סימטריות לכל $a, b \in \mathbb{Z}$, אם $(a, b) \in R_m$ אזי $(b, a) \in R_m$
- טרנזיטיביות לכל $a, b, c \in \mathbb{Z}$ אם $(a, b) \in \mathbb{R}_m$ וגם $(b, c)) \in R_m$ אז $(a, c) \in R_m$

3.0.3 <u>המסר מהמשפט השני:</u> ־ הגדרה: עבור $m \in \mathbb{Z}^+$ נגדיר $R_m := \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : a \equiv b(m)\}$

טענה ־ היחס R_m, הינו יחס שקילות.

<u>הוכחה</u> ־ נראה את התכונות הנ"ל:

- <u>רפלקסיביות:</u> נובע מיידית כי $m|a - a$ לכל a
- <u>סימטריות:</u> אם $a, b \in \mathbb{Z}$ אז $a \equiv b \pmod{m}$ אםם $b \equiv a \pmod m$
- <u>טרנזיביות:</u> אם a, b, c מתקיים: $m|a - b$ וגם $m|b - c$ צ"ל $m|a - c$:

$$m|\,(a - b) + (b - c) = a - c$$

3.0.4 הגדרה: יהי $m \in \mathbb{Z}^+$ קבוצה $x \subseteq \mathbb{Z}$ תיקרא מערכת שאריות שלמה עבור m (או מודלו m) אם $\forall y \in \mathbb{Z}\ \exists! x \in X :\ y \equiv x(m)$
= לכל $y \in \mathbb{Z}$ קיים $x \in X$ יחיד כך ש $y \equiv x\,(mod\ m)$

3.0.5 יהי $x \in \mathbb{Z}$ ויהיה $m \in \mathbb{Z}^+$ נסמן ב $[x]_m$ את מחלקת השקילות של $R_{\equiv m}$ שמכילה את x

רגע של מוטיבציה ־ למה אנו לומדים על קונגרואנציות?

1. RSA
2. האריטמתיקה שהמחשב משתמש בה הינה ארימתטיקה מודלארית

משפט: יהיה $m \in \mathbb{Z}^+$ ויהיו $a, b, c \in \mathbb{Z}$ וידוע ש $a \equiv b\,(m)$, אזי:

1. $a + c \equiv b + c\,(m)$
2. $a - c \equiv b - c(m)$
3. $ac \equiv bc(m)$

הוכחה ־ בבית. נראה את 3 :

- ידוע ש $m|a - b$ צ"ל $m|ac - b = c(a - b)$

משפט ־ אריטמתיקה מודלרית: יהי $m \in \mathbb{Z}^+$ ויהיו $a, b, c, , d \in \mathbb{Z}$ כך ש $a = b(m)$ וגם $c \equiv d(m)$

1. $a + c \equiv b + d(m)$
2. $a - c \equiv b - d(m)$
3. $ac \equiv bd(m)$

הוכחת 3 :

יש להראות כי $m|ac-bd$, מתקיים ש:

$$\begin{aligned} ac-bd &= ac-bc+bc-bd \\ &= c(a-b)+b(c-d) \\ &= kmc+lmb \\ &= m(kc+lb) \end{aligned}$$

ולכן $m|ac-bd=m(kc+lb)$

דוגמה:

$$\begin{aligned} 17 &\equiv 2(5) \\ 3 &\equiv 28(5) \\ 17\cdot 3 = 51 &\equiv 56(5) \equiv 2\cdot 26(5) \end{aligned}$$

חלוקה מודלררית - הבעיה:

$$\begin{aligned} 14 &\equiv 8(6) \\ 7\cdot \cancel{2 \equiv 2} &\cdot 4(6) \end{aligned}$$

משפט (חלוקה מודולרית): יהי $a,b,c\in\mathbb{Z}$ $m\in\mathbb{Z}^+$

$$ac\equiv bc(m) \iff a\equiv b\left(\frac{m}{gcd(c,m)}\right)$$

הוכחה

כיוון ראשון - $ac\equiv bc(m)\Rightarrow a\equiv b\left({}^{m}/_{gcd(c,m)}\right)$

- נניח כי $ac\equiv bc(\mod m)$ כלומר מתקיים ש: $m|c\left(a-b\right)$
- כלומר ישנו $k\in\mathbb{Z}e$ כך ש $cb-ca=c(b-a)=km$
- נגדיר $r=\frac{c}{gcd(c,m)}$ ונגדיר $s=\frac{m}{gcd(c,m)}$ עם $gcd\left(r,s\right)=1$
- ולכן ניתן לרשום:

$$\cancel{gcd\left(c,m\right)}\cdot r(a-b)=k\cdot\cancel{gcd(c,m)}\cdot s$$

- יכולנו לצמצם מכיוון שאנו בשלמים, ונקבל : $r(a-b)=k\cdot s$ כלומר $s|r(a-b)$
- מהאלגוריתם של אקולידם בעבור $gcd(s,r)=1$ נובע $s|a-b$
- כעת נציב חזרה את s , ונקבל: $\frac{m}{gcd(c,m)}|a-b \Leftrightarrow a\equiv b\left(\frac{m}{gcd(c,m)}\right)$, כנדרש.

כיוון שני - $ac\equiv bc(m)\Leftarrow a\equiv b\left({}^{m}/_{gcd(c,m)}\right)$

באופן סימטרי

מסקנות מתכונת החלוקה:

1. אם $gcd(c,m)=1$ אזי $ac\equiv bc(m)\iff a\equiv b(m)$

2. אם p ראשוני כך ש $p \nmid c$ אזי $a \equiv b(p) \iff ac = bc(p)$

<u>תרגיל:</u>

מצאו אם קיים מספר כך ש:

- אם מחלקים אותו ב 5 ומשאיר שארית 1
- אם מחלקים אותו ב 6 משאיר שארית 2
- אם מחלקים אותו ב 7 משאיר שארית 3

כלומר, נרצה למצוא $x \in \mathbb{Z}$ המקיים את מערכת המשוואות הבאה:

$$\begin{aligned} x &\equiv 1(5) \\ x &\equiv 2(6) \\ x &\equiv 3(7) \end{aligned}$$

בשלב זה נתמקד בפתרון משוואה אחת:

$$ax = b(m) \text{ עבור } a, b, \in \mathbb{Z} \text{ ו } m \in \mathbb{Z}^+$$

<u>דוגמה:</u> $2x \equiv 3(5)$ מתקיים בעבור $4, 9, \dots$ כלומר עם $k \in \mathbb{Z}$ אז הפתרון מתקיים לכל $4 + 5k$

<u>אבחנה:</u> אם $x_0 \in \mathbb{Z}$ מהווה פתרון ל $ax \equiv b(m)$ אז כל $y \in [x_0]_m$ מהווה פתרון, כלומר כל איבר במחלקת השקילות של x_0 מהווה פתרון למשוואה.

<u>הסבר לאבחנה:</u> את המשוואה $ax = b(m)$ אנו יכולים לרשום $ax = b - km$, וראינו בתרגולים (אלוגריתם אקולידס המרוחב) ש:

$$\begin{aligned} ax - km &= b \\ ax - xy &= b \end{aligned}$$

וראינו בהרצאות קודמות שמשוואה מהסוג $ax - km = b$ פתירה מעל Z אם"ם $(a, b)|b$, כלומר אין להריץ את האלגוריתם של אקולידס אם $(a, b)|b$ לא מתקיים.
ולכן...

<u>**משפט:**</u> **יהי** $m \in \mathbb{Z}^+$ **,** $a, b \in \mathbb{Z}$

1. **המשוואה** $a \equiv b(m)$ **פתירה אם"ם** $gcd\,(a, m)\,|b$
2. **אם פתירה אז יש לה** $gcd(a, m)$ **של פתרונות מודולו** m **שאינם קונגרואנטים אחד לשני**

<u>הוכחה:</u>

1. הוכחנו
2. נניח שפתירה ולכן:

- נניח כי $d := gcd\,(a, b)\,|b$
- ואם כך נפתור (מהתרגול) למשוואה $ax - my = b$ יש פתרונות בשלמים כאשר: $\begin{Bmatrix} x = x_0 + \left(\frac{m}{d}\right) t \\ y = y_0 + \left(\frac{a}{d}\right) t \end{Bmatrix}$ עם $t \in \mathbb{Z}$

- צ"ל שמספר מחלקות השקילות שווה בדיוק ל d.
- למה: יהיו: $\begin{Bmatrix} x_1 = x_0 + \left(\frac{m}{d}\right) t_1 \\ x_2 = x_0 + \left(\frac{m}{d}\right)_{t_2} \end{Bmatrix}$, זוג פתרונו שלמים, אזי

$$x \equiv x_2(m) \iff t_1 \equiv t_2(d)$$

הוכחה:

- יהיו $\begin{Bmatrix} x_1 = x_0 + \left(\frac{m}{d}\right) t_1 \\ x_2 = x_0 + \left(\frac{m}{d}\right)_{t_2} \end{Bmatrix}$ שני פתרונות כך ש $x_1 = x_2(m)$
- אז (1) מאריתמטיקה, ו (2) משפט החילוק המודלארי:

$$\begin{gathered} \cancel{x_0} + \left(\tfrac{m}{d}\right) t_1 \equiv \cancel{x_0} + \left(\tfrac{m}{d}\right) t_2(m) \\ \Downarrow (1) \\ \left(\tfrac{m}{d}\right) t_1 \equiv \left(\tfrac{m}{d}\right) t_2(m) \\ \Downarrow (2) \\ t_1 \equiv t_2 \left(\frac{m}{gcd(m,\frac{d}{m}}\right) \end{gathered}$$

- מסקנה מיידית מהלמה: נזדקק "לתת" ל t, d ערכים שונים על מנת לקבל את כל הפתרונות שאינם שקולים מודולו m, כנדרש.

שיעור 9 - 12/12/18

בשיעור שעבר:

- קונגרואנציות $a \equiv b(m)$ אם $m|a-b$
- אריתמטיקה מודולארית - למשל $a \equiv b(m), c \equiv d(m) \Leftarrow ac \equiv bd(m)$
  - באמצעות משפט שכזה אפשר להוכיח שאם $a \equiv b(m)$ אז $a^k \equiv b^k(m)$ בגלל שזה $a \equiv b(m) \iff aa \equiv bb(m)$
- בחלוקה ראינו שזה בעייתי, והוכחנו ש $a \equiv b\left(\frac{m}{gcd(c,m)}\right) \iff ac \equiv bc(m)$
- הראינו כיצד פותרים משוואה יחידה $ax = b(m)$:
  1. $ax = b(m)$ פתירה $\iff gcd\left(a,m\right)|b$
  2. אם פתירה $\Leftarrow$ אז ישנם $gcd(a,m)$ פתרונות שונים למושוואה מודולו m
- והיום נראה כיצד פותרים מספר משוואות - לשם כך:
  - נציג מהו הופכי מודולארי
  - משפט השאריות הסיני

הופכי מודולארי:

ב $\mathbb{Z}$ אנו רואים $x + (-x) = 0$
ב $\mathbb{R}$ אנו רואים $x \cdot x^{-1} = x \cdot \frac{1}{x} = 1$
נרצה לחקות מנגנון זה
ראינו שאם $gcd(a,m) = 1$ אז $ax = 1(m)$ יש פתרון יחודי מודלו m

3.0.6 הגדרה: יהיו $m \in \mathbb{Z}^+$, $a \in \mathbb{Z}$ כך ש $gcd(a,m) = 1$ a הינו הופכי מודולארי ל a מודולו m אם $a \cdot \widetilde{a} = 1(m)$

במילים אחרות: $[a]_m \overset{\text{mod'}}{\cdot} [\tilde{a}]_m = 1$

דוגמאות:

1. מיהו ההופכי המודולארי של של $[7]_{31}$?

   על בסיס מה שלמדנו אנו מחפשים את הפתרון למשוואה $7x = 1(31)$?

   תשובה: 9 הוא הופכי ל 7 מודולו 31 או במלים אחרות $[7]_{31}\,[9]_{31} = 1$

2. מיהו ההופכי של $[5]_{10}$?

   לא עומד בתנאי ההגדרה

3. מיהו ההופכי של $[0]_m$?

   לא קיים.

<u>אבחנה:</u> p ראשוני. נניח ש $a \in [1, p-1]$ אז לכל a שכזה קיים הופכי מודולו p. כאשר $gcd(a,p) = 1$ אז $p \nmid a$

<u>הוכחה:</u> $ax \overset{?}{\equiv} 1(p)$ אם $gcd(a,p) = 1$

4. $6^2 \equiv 36 \equiv 1(5)$ כרגע אמרנו ש 6 הופכי לעצמו מודלו 5, כי $6x = 1(5)$ ונציב $x = 6$

3.0.7 הגדרה: יהיו $m \in \mathbb{Z}^+$, $a \in Z$ כך ש: $gcd(a,m) = 1$ נאמר ש a הופכי לעצמו מודולו m אם $a^2 = 1(m)$

משפט: יהי p ראשוני והי $a \in \mathbb{Z}$ כך ש $gcd(a,p) = 1$ אז a הופכי לעצמו מודולו p $\iff$ $a = 1(p)$ או $a \equiv -1(p) \equiv p-1(p)$

canon	0	**1**	2	3	4	$\cdots$ $\cdots$	$\boldsymbol{p-1}$
inverse	/	**1**					$\boldsymbol{p-1}$

<u>הוכחה:</u>

<u>כיוון ראשון:</u>

- אם $a \equiv \pm 1(p)$ אז $a^2 \equiv (\pm 1)^2\,(p)$ כלומר $a^2 \equiv 1(p)$ וסיימנו

<u>כיוון שני:</u>

- נניח בכיוון שני $a^2 \equiv 1(p)$, ולכן:

$$p | a^2 - 1 = (a-1)(a+1)$$

- היות ו p ראשוני אז:

$$p|a+1 \Leftrightarrow a \equiv -1(p) \text{ או } p|a-1 \Leftrightarrow a \equiv 1(p)$$

$\square$

<u>תרגיל:</u>

יהי $p \geq 3$ ראשוני ויהי $gcd(a,p)=1$ הראו כי a הופכי לעצמו מודולו p^k אס"ם $a \equiv \pm 1(p)$

דוגמאות:

- $p=3$

canon	0	**1**	**2**
inverse	/	**1**	**2**

- $p=5$

canon	0	**1**	2	3	**4**
inverse	/	**1**	3	2	**4**

- $p=7$

canon	0	1	2	3	4	5	6
inverse	/	1	4	5	2	3	6

- $p=11$

canon	0	1	2	3	4	5	6	7	8	9	10
inverse	/	1	6	4	3	9	2	8	7	5	10

כעת נחזור למערכת המשוואות שלנו: $\begin{Bmatrix} x \equiv 1(5) \\ x \equiv 2(6) \\ x \equiv 3(7) \end{Bmatrix}$ ונרצה למצוא $x \in \mathbb{Z}$ המקיים את המערכת.

משפט השאריות הסיני: יהיו $n_1, n_2, ..., n_r$ מספרים שלמים חיוביים שזרים בזוגות אזי למערכת $\begin{Bmatrix} x \equiv a_1(n_1) \\ x \equiv a_2(n_2) \\ \vdots \\ x \equiv a_r(n_r) \end{Bmatrix}$ קיים פתרון יחיד מודלו

$\prod_{i=1}^{r} n_i$

ראינו בתרגול שאם $\gcd(a,b) \cdot \operatorname{lcm}(a,b) = a \cdot b$ כאשר $lcm\left(n_1, n_2, ..., n_r\right) = \prod_{i=1}^{r} n_i$

<u>הוכחה:</u>

<u>קיום:</u>

- נגדיר $x := \sum_{i=1}^{r} a_i M_i y_i$
  - כאשר a_i נתון.
  - $M_i := \frac{\prod_{i=1}^{r} n_k}{n_i} = \frac{n_1 \cdot n_2 \cdot ... \cdot \cancel{n_i} \cdot ... \cdot n_r}{\cancel{n_i}}$,

- ההופכי המודולארי של M_i מודולו $y_i = n_i$, y_i קיים ואכן $gcd(M_i, n_i) = 1$

- נותר להראות ש x שהגדרנו פותר את המערכת:

  נבחר $k \in [r]$ ונראה ש: $x \equiv a_k\ (n_k)$, נרשום:

$$x = \sum_{i=1}^{r} a_i M_i y_i = \underbrace{a_1 M_1 y_1}_{n_k \in} + \underbrace{a_2 M_2 y_2}_{n_k \in} + ... + a_k M_k y_k + ... + \underbrace{a_r M_r y_r}_{n_k \in} \equiv a_k\ (n_k)$$

$$\iff\ 0(n_k) + 0(n_k) +,,, + a_k M_k y_k + ... + 0(n_k) = a_k M_k y_k \equiv a_k(n_k)$$

- נותר להוכיח $a_k M_k y_k \equiv a_k(n_k)$ אבל מכך שצמצמנו את n_k מתקיים:

$$a_k M_k y_k \equiv 1(n_k)$$

<u>יחידות:</u>

- נניח בשלילה שישנם x_1, x_2 פתרונות למערכת כך ש: $x_1 \not\equiv x_2 \left(\prod_{i=1}^{r} n_i\right)$

- אם כך לכל $k \in [r]$ מתקיים $x_1 \equiv x_2 \equiv a_k(n_k)$

- ולכן לכל $k \in [r]$ מתקיים $n_k | \underbrace{x_1 - x_2}_{=m}$

  - הראינו בתרגול: אם $n_1, n_2, ..., n_r$ זרים בזוגות ובנוסף : $\forall i \in [r] :\ n_i | m$ אזי $\left(lcm(n_1, n_2, ..., n_r) = \prod_{i=1}^{r} n_i\right) | m$

- לפי המשפט מהתרגול :

$$n_1 n_2 \cdot .... \cdot n_r | x_1 - x_2 \Rightarrow x_1 \equiv x_2\ (n_1 n_2 \cdot .... \cdot n_r)$$

וזו סתירה.

<u>תרגיל:</u>

$$6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6(7) \equiv 1 \cdot (2 \cdot 4) \cdot (3 \cdot 5) \cdot 6(7) \equiv 1 \cdot (1(7)) \cdot (1(7)) \cdot 6(7)$$

$$\equiv 6 \equiv -1(7)$$

<u>ובהכללה:</u>

$$(p-1)! \equiv 1 \cdot 2 \cdot ....(p-1)\ (p) \equiv p - 1(p) \equiv -1(p)$$

וזו הוכחת המשפט....

משפט $(wilson)$ **: יהיה** p **ראשוני אזי** $(p-1)!\equiv -1(p)$

משפט (הפוך $wilson$ **) : אם** $(n-1)!\equiv -1(n)$ **אז** n **ראשוני.**

<u>הוכחה:</u>

נניח בשלילה ש n פריק , כלומר $n=a\cdot b$, $2\le a,b<n$, ובנוסף $(n-1)!\equiv -1(n)$

<u>נביט על a, מתקיים:</u>

- היות ו $a<n$ נובע ש: $a<n\Rightarrow a|\,(n-1)!$
- היות ו $n|\,(n-1)!+1$ ו $a|n$ אז $a|\,(n-1)!+1$
- ולכן $2\le a|\,[((n-1)!+1)+(n-1)!=1]$, וזו סתירה.

שיעור 10 - 19/12/18

בשבוע שעבר:

- קונגרואציות $a\equiv b(m)$ אם $m|a-b$
- התעניינו במערכות משוואת מהסוג $ax\equiv b(m)$
- משפט השאריות הסיני שהנתן מערכת משוואות, נבחר את $x=\sum a_iM_iy_i$
- הופכי מודולארי אם $gcd(a,m)=1$ אז $ax\equiv 1(m)$
- $wilson$: n ראשוני $\iff n-1\equiv -1(n)$

דוגמה: יהיה $p=5$

$$\begin{array}{cc} \{1,2,3,4\} & \\ \downarrow & \times 2 \\ \{2,4,6,8\} & \end{array}$$

נבחן את שקרה:

1. 0 "לא נולד"
2. לא איבדנו אף נציג

דוגמה 2 - נכליל:

יהיה p ראשוני כלשהו:

$$\begin{array}{cc} \{1,2,3,4,...,p-1\} & \\ \downarrow & \times a\ gcd(a,p)=1 \\ \{a,2a,3a,...,(p-1)a\} & \end{array}$$

הוכחה -"0 לא נולד" :

- נניח בשלילה כי קיים $k\in[1,p-1]$ כך ש $p|ak$, היות ו p לא מחלק את k , וגם p לא מחלק את k נובע ש $p\nmid a\cdot k$

הוכחה: "לא אבדנו אף נציג":

- לכאורה צ"ל $\{a,2a,3a,...,(p-1)a\}\equiv\{1,2,3,4,...,p-1\}$ אבל זה שיווון בין קבוצות קונגוראנטיות וזה מסובך, ולכן:

- צ"ל: $a(2a)(3a).....(p-1)(a) \equiv 1 \cdot 2 \cdot 3....(p-1) \mod p$
- נניח בשלילה שיש $k_1, k_2 \in [p-1]$ כך ש $k_1 \neq k_2$ (כלומר $k_1 \not\equiv k_2\ (p)$ כך שעבורם $ak_1 \equiv ak_2\ (p)$, k_1, k_2 זרים זה לזה, ולכן ממשפט החילוק המודולארי $\cancel{a}k_1 \equiv \cancel{a}k_2\ (p)$, כנדרש.

מה קיבלנו?

$$a(2a)(3a).....(p-1)(a) \equiv (p-1)! \mod p$$
$$(a)^{p-1}(p-1)! \equiv (p-1)! \mod p$$

מכך ש : $gcd\left((p-1)!, p\right) = 1$, נובע שניתן לצמצם ונקבל:

$$a^{p-1} \equiv 1(p)$$

וזו הוכחת משפט פרמה הקטן: יהי p ראשוני ויהי $gcd(a,p)=1$ אז $a^{p-1} \equiv 1(p)$

או בניסוח אחר: יהי p ראשוני, והיה $a \in \mathbb{Z}$ אזי $a^p \equiv a(p)$

הוכחה הניסוח:

ינפצל למקרים:

- אם $p \nmid a$ אז מפרמה הקטן $a^{p-1} \equiv 1(p) \Leftarrow a^p \equiv a(p)$
- אם $p|a$ אז $p|a^p$ ואז נקבל $\begin{matrix} a \equiv 0(p) \\ a^p \equiv 0(p) \end{matrix} \Leftarrow a^p \equiv a(p)$

<u>תרגיל:</u> מהי השארית הקנונית של 3^{201} מודולו 11 כלומר $\left[301^{201}\right]_{11}$?

<u>פתרון:</u>

$$3^{10} \overset{\text{Fermat}}{\equiv} 1(11) \to \left(3^{10}\right)^{20} \equiv 1(11)$$
$$\Downarrow$$
$$3 \cdot \left(3^{10}\right)^{20} \equiv 3(11)$$
$$\Downarrow$$
$$\left[3^{201}\right]_{11} = 3$$

תרגיל: הוכיחו כי $a^{21} \equiv a(15)$ לכל $a \in \mathbb{Z}$ (הבעיה 15 לא ראשוני)

נזכר כי $\begin{matrix} a \equiv b(n_1) \\ a \equiv b(n_2) \\ gcd(n_1, n_2) \end{matrix} \Rightarrow a \equiv b \cdot gcd(n_1, n_2)$

אז נחשב:

1. $a^{21} \equiv a(3)$

$$a^3 \overset{\text{Fermat}}{\equiv} a(3) \to \left(a^3\right)^7 \equiv a^7(3)$$

$$a^7 \equiv a \cdot a^6 \to a\left(a^3\right)^2 \equiv a \cdot a^2 \equiv a^3 \equiv a(3)$$

2. $a^{21} \equiv a(5)$

$$a^5 \overset{\text{Fermat}}{\equiv} a(5) \to \left(a^5\right)^4 \equiv a^4(5) \to a\left(a^5\right)^4 \equiv a^5 \equiv a(5)$$

שאלה: האם 63 ראשוני?

אם נמצא עכשיו a כך ש: $a^{63} \not\equiv a(63)$, אז נוכל לומר ש 63 איננו ראשוני. $2^6 \equiv 64 \equiv 1(63)$

$$2^{63} \equiv 2^3 2^{60} \equiv 2^3 \left(2^6\right)^{10} \equiv 2^3 \cdot 1^{10}(63) \equiv 2^3(63) \to 2^{63} \not\equiv 2(63)$$

כלומר הראנו $\neg b \to \neg a$כלומר הראנו בa אינו קונגראנטי ל 1 ומכאן שאינו ראשוני, השאלה האם ניתן "לעבוד" על פרמה הקטן

שאלה: האם $341 = 11 \cdot 31$

1. האם $2^{340} \equiv 1(11)$

$$2^{10} \overset{\text{Fermat}}{\equiv} 1(11) \to \left(2^{10}\right)^{34} \equiv 1(11)$$

2. $2^{340} = 1(31)$

$$2^5 = 32 \overset{\text{Fermat}}{\equiv} 1(31)$$

$$2^{340} \equiv \left(2^5\right)^{68} = 1(31)$$

יהיה $2^{340} \equiv 1(341)$

3.0.8 הגדרה: מספר n פריק יקרא פסואדו־ראשוני מבסיס b אם $b^n \equiv b(n)$

דוגמה 341 הינו פסודו־ראשוני מבסיס 2

תרגיל בית:הראו ש 91 הינו פסודו ראשוני מבסיס 3

דוגמה: הראו ש 341 איננו פסודו־ראשוני מבסיס 7 . המטרה: $7^{340} \equiv 1(341)$

$$
\begin{gathered}
7^3 \equiv 343 \equiv 2(341) \\
7^{340} = \left(7^3\right)^{113} 7 \equiv 2^{113} \cdot 7 \\
but: \\
2^{10} = 1024 \equiv 1(341) \\
so: \\
2^{113} \cdot 7 \equiv 2(2^{10})^{11} 2^3 \cdot 7 \equiv 1(341)
\end{gathered}
$$

מספרים זדוניים:

561=3·11·17

נבחר a כך ש $gcd\left(a, 561\right) = 1$ ולכן $gcd(a,3) = gcd(11) = gcd(17) = 1$ כלומר אנו יודעים ש:

$$a^2 = 1(3) \qquad a^6 \equiv 1(11) \qquad a^{16} \equiv 1(16)$$

$$a^{560} \equiv a^{2^{280}} \equiv 1(3)$$

$$a^{560} \equiv a^{10^{56}} \equiv 1(11)$$

$$a^{560} \equiv a^{16^{25}} \equiv 1(17)$$

3.0.9 הגדרה: מספר פריק n כך ש $b^{n-1} \equiv 1(n)$ לכל $b \in \mathbb{Z}$ כך ש : $gcd(b,n)=1$ נקרא מספר $Car-Michael$ קרמייקל.

משפט: יהיה $n = q_1 q_2 \cdot ..... \cdot q_k$ **כאשר** $\{q_i\}_{i=1}^k$ **ראשוניים, ובנוסף** $\forall j \in [k]$ **אם** $q_j - 1 | n-1$ **אז** n **הינו** $Car-Michael$

הוכחה:

- יהי n כמו במשפט, והי $b \in \mathbb{Z}$ כך ש $gcd(b,n)=1$, יש להראות ש : $b^{n-1} \equiv 1(n)$
- היות ו $gcd(b,n)=1$ אז: $\forall j \in [k]$ מתקיים $(b,q_j)=1$ ולכן $\forall j \in [k]$ מתקיים

$$b^{q_j-1} \overset{\text{Fermat}}{\equiv} 1(q_j)$$

- בנוסף מהנתון לכל $j \in [k]$ מתקיים:

$$n-1 = t_j(q-1)$$

עבור $t_j \in \mathbb{Z}$.

- ולכן לכל $j \in [k]$

$$b^{n-1} \equiv b^{t_j(q_j-1)} \equiv \left(b^{q_j-1}\right)^{t_j} \equiv 1(q_j)$$

$$b^{n-1} \equiv 1\,(q_1 q_2 \cdot ..... \cdot q_k) = 1(n)$$

שיעור 11 - 26/12/18

רקע: משפט פרמה עוזר חשב שקילויות בהן המודלו ראשוני. משפט $Euler$ יסייע בחישוב שקילויות בה המודולו פריק או ראשוני, ולכן זוהי הכללה של משפט פרמה.

3.0.10 הגדרה: יהי $n \in \mathbb{Z}^+$. נרשום $\varphi(n)$ בתור כמות המספרים הטבעיים הקטנים מ n שזרים אליו כלומר

$$\varphi(n) = |\{k \in [n] :\ gcd(k,n)=1\}|$$ (פונקציה כפלית)

משפט $Euiler$: עבור $n \in \mathbb{Z}^+$ ויהי a כך ש $gcd(a,n)=1$ אז $a^{\varphi(n)} \equiv 1(n)$

דוגמה: המספרים הראשונים עד מספר n כלשהו

$$\begin{array}{lll} \varphi(1)=1 & \boldsymbol{\varphi(2)=1} & \boldsymbol{\varphi(3)=2} \\ \varphi(4)=2 & \boldsymbol{\varphi(5)=4} & \varphi(6)=2 \\ \boldsymbol{\varphi(7)=6} & \varphi(8)=4 & \end{array}$$

אבחנות:

1. לכל $n \in \mathbb{Z}^+ \backslash \{1\}$ $\varphi(n) \leq n-1$,
2. לכל n פריק $\varphi(n) \leq n-2$

$$\varphi(n) = n = 1 \iff n \text{ ראשוני}$$

דוגמא: יהיה $n=8$ אז:

$$\mathbf{1} \quad \underline{3} \quad \mathit{5} \quad 7 \quad \to \text{Coprime integers to } 8$$

$$\times 3$$

$$gcd(3,8)=1 \quad \underline{3} \quad \mathbf{9} \quad 15 \quad \mathit{21}$$

כמו שראינו בפרמה הקטן, ע"י הכפלה ב 3 לא "איבדנו" אף נציג, ולא נולד 0 . כעת נמשיך במטרתנו מציאת אלגוריתם למציאת ראשוניים.

3.0.11 הגדרה: יהי $n \in \mathbb{Z}^{+}$, מהי $A \subseteq \mathbb{Z}$ כך ש $|A| = \varphi(n)$ כך שזו מקיימת:

1. כל $a \in A$: $gcd(a,n) = 1$
2. כל איברי A אינם קונגוראנטים אחד לשני מודלו n , אזי זו תקרא **מערכת שאריות מצומצת** מודלו n

דוגמה: $n = p$ ראשוני $\{1, ..., p-1\}$

משפט: יהי $n \in \mathbb{Z}^{+}$ ותהי $\{r_1, r_2, ..., r_{\varphi(n)}\}$ מערכת שאריות מצומצת מודלו n . והיה $a \in \mathbb{Z}$ כך ש $gcd(a,n) = 1$, אזי $\{ar_1, ar_2, ..., a_{r\varphi(n)}\}$ הינה גם מערכת שאריות מצומצמת מדולו n

הוכחה: ־ הרעיון נוכיח באמצעות הזרות של המספרים

- עבור א': יהי $j \in [\varphi(n)]$, ונשקול את ar_j אז $gcd(ar_j, n) = 1$ ־ מהמשפט היסודי של הארימתטיקה שאם אין בין a, n פקטורים משותפים אז גם בין ar_j, n אין פקטורים משותפים
- עבור ב': יהי r_i ו r_j הקבוציה המקורית כך ש $i \neq j$. נניח בשלילה ש $ar_i \equiv ar_j(n)$ וזו סתירה להגדרה של הקבוצה ממנו לקחנו את r_i ו r_j .

הפונקציה נקראת $\varphi(\cdot)$ נקראת Euler's totient function

הוכחת אוילר:

מה נרויח אם נוכיח: תהי $r_1, r_2, ...r_{\varphi(n)}$ מערכת שקילויות מצומצת מודלו n ,אז לפי המנוע החדש מתקיים:

$$(ar_1)(ar_2)...(ar_{\varphi(n)}) \equiv r_1 r_2 ....r_{\varphi(n)}(n)$$

$$a^{\varphi(n)}(r_1, r_2......r_{\varphi(n)}) \equiv r_1 r_2 ....r_{\varphi(n)}(n)$$

$$a^{\varphi(n)} \equiv 1(n)$$

שאלה: ראינו שלכל p ראשוני $\varphi(p) = p - 1$, מהי $\varphi(p^2)$? מהי $\varphi(p^k)$

הוכחה:

$$\varphi(p^k) \overset{\text{def } \varphi}{=} \left|\left\{x \in [p^k] : \ gcd(x, p^k) = 1\right\}\right| = \left|[p^k] \setminus \left\{x \in [p^k] : \ p|x\right\}\right| \overset{\text{def } p|x}{=} \left|[p^k] \setminus \left\{a \cdot p : \ a \in [p^{k-1}]\right\}\right|$$

$$\left|[p^k] \setminus \left\{p, 2p, ...p^{k-1} \cdot p\right\}\right| = p^k - p^{k-1} = p^k\left(1 - \tfrac{1}{p}\right)$$

שערו בנפשכם שאנו נוכיח של φ יש תכונה:

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$$

כאשר $gcd(m,n) = 1$.

באופן כללי, נאמר $f : \mathbb{Z} \to \mathbb{Z}$: כך ש: $f : (m \cdot n) = f(m) \cdot f(n)$

בכלל עם ש $gcd(m,n) = 1$ נקראת <u>כפליות</u>, נניח שהוכחנו φ כפלית איך זה עוזר ל חשב $\varphi(n)$ עבור n שרירותי? תנו לי n ויש לי פיקטור:

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

אז:

$$\varphi(n) = \varphi(p_1^{a_1} \cdot p_2^{a_2} \cdot .... \cdot p_k^{a_k}) = \varphi(p_1^{a_1}) \cdot \varphi(p_1^{a_1}) \cdot .... \cdot \varphi(p_k^{a_k})$$

$$= p_1^{a_1}\left(1 - \frac{1}{p_1}\right) p_2^{a_2}\left(1 - \frac{1}{p_2}\right) \cdot ... \cdot p_k^{a_k}\left(1 - \frac{1}{p_k}\right) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot ... \cdot \left(1 - \frac{1}{p_k}\right)$$

זה מה שנקבל אם נוכיח את הכיפליות

טענה: φ הינה כפלית

לשם כך ניזכר בשתי תכונות אותן הוכחנו בשיעורים קודמים:

1. $gcd(a,bc)=1 \iff gcd(a,b)=1 \wedge gcd(a,c)=1$
2. $gcd(qm+r)=gcd(r,m)$

<u>הוכחה:</u>

$$\varphi(m\cdot n)=|\{x\in[m\cdot n]:\ gcd(x,mn)=1\}|\overset{1}{=}\varphi(m\cdot n)=|\{x\in[m\cdot n]:\ gcd(x,m)=1\wedge gcd(x,n)=1\}|$$

<u>הצעה:</u> להוכיח בשני שלבים

שלב א: נאסוף את כל המספרים ב $[m,n]$ שזרים ל n

שלב ב: מבין כל מי שאספנו נשמר רק את אלו שזרים ל n

נסדר את המספרים במטריצה $n\times m$

$$\begin{array}{cccccc}
\mathbf{1} & \mathbf{2} & \boldsymbol{\cdots} & \boldsymbol{r} & \boldsymbol{\cdots} & \boldsymbol{m}\\
m+1 & m+2 & \cdots & \boldsymbol{m+r} & \cdots & 2m\\
2m+1 & 2m+2 & \cdots & \boldsymbol{2m+r} & \cdots & 3m\\
\vdots & \vdots & & \vdots & & \vdots\\
(n-1)\,m+1 & (n-1)\,m+2 & \cdots & \boldsymbol{(n-1)\,m+4} & \cdots & nm
\end{array}$$

בשורה: $m\quad\cdots\quad r\quad\cdots\quad 2\quad 1$ יש $\varphi(m)$ מספרים זרים ל m

בהנתן עמודה זרה ל m כלשהי: $\begin{array}{c}\boldsymbol{r}\\ \boldsymbol{m+r}\\ \boldsymbol{2m+r}\\ \vdots\\ \boldsymbol{(n-1)\,m+4}\end{array}$ ישנן $\varphi(n)$, לפי תזכורת 2.

יהי $r\in[m]$, כך ש $gcd(r,m)=1$, נניח בשלילה שישנם $q_1,q_2\in[0,n-1]$ כך ש $q_1\neq q_2$ ולכן $q_1\not\equiv q_2(n)$ ונניח בשלילה ש:

$$q_1\cancel{m}+\cancel{r}\equiv q_2\cancel{m}+\cancel{r}\,\cancel{(n)}$$

נתון לצמצם כי מנתון שהם זרים.

RSA

מבוא קצר לקריפטוגרפיה:

- הצפנת הודעות: נניח ש $Alice$ שולחת הודעה m ל Bob ואנחנו רוצים ש Eve לא תצליח לקרוא את הדברים הבאים:
  - אלגוריתם הצפנת ההודעה m להודעה c בקלות
  - של Eve יהיה קשה מאוד לפענח את ההודעה
  - של Bob יהיה אלגוריתם פשוט לפענח את c ל m
- חתימה דיגיטלית:

- היא האפשרות ש $Alice$ "תחתום" על ההצפנה שלה, והמחשב ידע לזהות ניסיון פענוח עם החתימה הלא נכונה
- של bob יהיה את החתימה הנכונה

ישנן שתי גישות מרכזיות בקריפט' למימוש ה app הללו:

- public key encryption
- private key encryption
  - ההודעות בנויות מאותיות מתוך קבוצה בשם $\sum$
  - ב key הכוונה לפנוקציה $f:\sum\to\sum$
  - ולכן אם ל $Alice$ יש פונקציה S שמצפינה באופן כלשהי, אז באמת נצליח להסתיר מ Eve את ההודעה
  - הבעיה היא איך מעבירים את S ל bob
    * פתרון אחד: ישנו אחד גדול, ו$Alice$ ו Bob יודעים ללכת לבקש ממנו
    * פתרון שני RSA: ישנן שתי מפתחות שמיוצרים יחדיו :
      · $P_A = \text{public key}$
      · $S_A = \text{secert key}$
      · שיתנהגו כך $m = P_A\left(S_A(m)\right) = S_A\left(P_A\left(m\right)\right)$
  - אם כן, איך עושים חתימה דיגטלית עם

שיעור 12 - 02/01/19

חזרה על רעיונות ה RSA , והחתימה הדיגטלית

קריפטו מבוססת תורת המספרים

בעצם אנחנו רוצים:

$$P_A(S_A(m) = m = S_A\left(P_A(m)\right)$$

האלגוריתם:

- פלט S,P

1. מצא שני ראשוניים p ו q "ענקיים"
2. קבע $n := p\cdot q$
3. מצא מספר אי־זוגי e כך שמתקיים $gcd\left(e,\varphi(n)\right)=1$
4. קבע d להיות ההופכי של e במודלו $\varphi(n)$
5. פלט: מפתח ציבורי:= $\langle e,n\rangle$. מפתח פרטי:= $\langle d,n\rangle$

- מהם אם כך P ו S ? $\forall m_{\text{a letter}} \in \left\{[0]_n,[1]_n,\dots[n-1]_n\right\}$ נגדיר $P(m)=m^e(n)$, $S(m)=m^d(n)$

טענה: לכל $m\in[0,n-1]$ **מתקיים ש:** $P_A(S_A(m)=m=S_A\left(P_A(m)\right)$

<u>הוכחה:</u>

1. נראה ש $P_A(S_A(m)=(P_A(m))$:

$$P(S(m))\overset{def}{=}\left[(S(m))^e\right]_n\overset{con}{=}\left[\left(m^d\right)^e\right]_n=\left[m^{de}\right]_n=\left[\left(m^e\right)^d\right]_n=\left[P\left(m\right)^d\right]_n=S(P(m))$$

2. יש להראות $\forall m\in[0,n-1]$, $m^{ed}\equiv[m]_n$

- היות ו $n=pq$ <u>צ"ל:</u> $m^{ed}\equiv[m]_{pq}$
- ממשפט השאריות הסיני מספיק להוכיח: 1. $m^{ed}\equiv[m]_p$. 2. $m^e\equiv[m]_q$. נוכיח את 1 , 2 זהה:
- ידוע ש $ed\equiv[1]_{\varphi(n)}$
- אבל $\varphi(n)=\varphi(qp)=\varphi(p)\varphi(q)=(p-1)\left(q-1\right)$
- ואם כך: $ed\equiv1+k\left(p-1\right)\left(q-1\right)$ $(*)$ כעת ניגש להוכחת 1 : $m^{ed}\equiv[m]_p$: $\forall m\in[0,n01]$
  - עבור $m\equiv[0]_p$ הטענה נכונה.
  - נניח אם כך ש $m\not\equiv[0]_p$
  - כעת:

$$m^{ed}\overset{*}{=}m^{1+k(p-1)(q-1)}=m\cdot m^{k(p-1)(q-1)}=m\cdot m^{(p-1)^{k(q-1)}}$$

  - היות ואנו במקרה שבו $m\not\equiv[0]_p$ נדע שהנציג הקנוני לmצודולו p נלקח מ $[1,p-1]$ נקרא לו z , אם כך נוכל לרשום ש:

$$m^{ed}\equiv m\left(z^{p-1}\right)^{k(q-1)}(mod\ p)\overset{Fermat}{\equiv}m(mod\ p)$$

$\square$

המבחן

- מבנה המבחן: יפורסם בהמשך
- השאלות פחות או יותר ברמת המטלות
- אין דף נוסחאות
- המבחן 3 שעות

שיעור 13 - 09/01/18

המבחן

1. בקיאות בסיסית 60-65
2. בקיאות + הוכחות אבסטרקטיות 20-25
3. יצרתיות 10-15

השאלות משבוע שעבר:

1. <u>הגדירו gcd של שני מספרים באמצעות המשפט היסודי של הארימתטיקה:</u>

- נגדיר $a=p_1^{a_1}p_2^{a_2},.....p_k^{a_k}$

- נגדיר $b == p_1^{b_1} p_2^{b_2}, ...p_k^{b_k}$
  - כאשר $a_i, b_i \geq 0$ לכל $i \in [n]$
- כעת נגדיר $gcd(a,b) = \prod_{i=1}^{k} min\,(a_i, b_i)$

2. יהיו $n \in \mathbb{Z}$ $a \in [1, n-1]$ הוכיחו כי $gcd(a,n) = gcd(n-a, n)$:

- המנוע של $euclid$: $gcd(a,b) = gcd(a+cb, b)$

פתרון:

- ראשית $d|a$ וגם $d|n$ לכן $d|n-a$
- אצלנו $d|n-a$, $d|n$ לכן $d|n = n-(n-a)$

3. השתמשו בחלק הקודם על מנת להוכיח ש$\varphi(n)$ לכל $n \geq 3$

- מהגדרה $S = \{x \in [n] : (a,n) = 1\}$ זוהי $\varphi(n)$
- נגדיר את הקבוצה $\left\{\langle a, n-a\rangle :\ gcd(a,n) = 1, a < \frac{n}{2}\right\}$, למעשה יצרנו זוגות של מספרים הזרים ל n , שלפי סעיף קודם מכיל שני איברים מ S
- ניתן להראות שכל זוג מכיל שני איברים שונים.
- נותר לבדוק את המקרה של $\frac{n}{2}$ - ואז $n-a = a$
  - אם n איזוגי - $n/2$ אינו מספר שלם, ואינו רלוונטי לקבוצה
  - אם n זוגי - אז $gcd(\frac{n}{2}, n) \neq 1$
- ולכן חילקנו את איברי הקבוצה S לזוגות, ולכן $\varphi(n)$ הינה זוגית
- נותר להראות שזה לא עובד ל1,2 וכן עובד ל3 , וסיימנו

4. הוכיחו כי $\forall n \geq 2\ ,\ \sum a = \frac{n\varphi(n)}{2}$

- $2\sum_{a \in S} a + \sum_{a \in S} n-a = \sum_{a \in S} n = n\sum_{a \in S} 1 = n|S| = n\varphi(n)$
- צריך להראות שבאמת $\sum_{a \in S} a = \sum_{a \in S} n-a$ (הראה בע"פ)

5. ספקו הוכחה נוספת לטענה ש $\varphi(n)$ זוגית לכל $a \geq 3$ ללא שימוש בחלק 2 שיקלו 2 מקרים:

- ל n יש פקטור אי־זוגי
- ל n אין פקטור אי־זוגי

תשובה:

- אם ל n יש פקטור אי־זוגי p א ניתן $n = p^k \cdot m$ כאשר $gcd(p^k, m) = 1$ עבור $k \in \mathbb{Z}^+$
- ולכן $\varphi(n) = \varphi(p^k m) = \varphi(p^k)\varphi(m) = p^{k-1}\,(p-1)\,\varphi(m)$ ו $p-1$ זוגי
- אחרת אם ל n אין פקטור אי־זוגי אז $n = 2^k$, והיות ו $n \geq 3$ אז $k \geq 2$
- לכן $\varphi(n) = \varphi(2^k) = 2^{k-1}(2-1) = 2^{k-1}$

6. הוכיחו כי אם $a \equiv b(n)$ אז $gcd(a,n) = gcd(b,n)$

- נראה ש $d|a$ וגם $d|n$ אז $d|b$
  - $b = kn$
  - $a = nk_1 + r$ ו $b = nk_2 + r$ והצבת ב r : $b = n \cdot k_2 - nk_1 + a = (k_2 - k_1)\,n + a$
- צד שני סימטרי

7. <u>האם ההפך נכון? כלומר אם $gcd(a,n)=gcd(b,n)$ אז $a\equiv b(n)$?</u>

$$n=10,a=2,b=6$$

$$gcd(2,10)=2,gcd(6,10)=2,2\not\equiv 6(10)$$

8. <u>יהיו x,y אי־זוגיים הראו כי x^2+y^2 זוגי אך $4-x^2+y^2$</u>

- נכתוב $x=2k+1$ ו $y=2l+1$

$$x^2+y^2=(2k+1)^2+(2l+1)^2=..=4\,(???)+2$$

9. <u>הראו ש : $gcd\left(F_{n+2},F_{n+1}\right)=gcd\left(F_{n+1},F_n\right)$, כאשר F_i הינו מספר הפיבונאצי ה i</u>

- מאוקלידס:

$$gcd\left(F_{n+2},F_{n+1}\right)=gcd\left(F_{n+1}+F_n,F_{n+1}\right)=gcd\left(F_{n+1},F_{n+2}-\left\lfloor\frac{F_{n+2}}{F_{n+1}}\right\rfloor F_{n+1}\right)=$$
$$=gcd\left(F_{n+1},F_{n+2}-\left\lfloor 1+\frac{F_n}{F_{n+1}}\right\rfloor,F_{n+1}\right)=gcd\left(F_{n+1},F_{n+2}-F_{n+1}\right)=gcd\left(F_{n+1},F_{n+2}-\left\lfloor\frac{F_{n+1}+F_n}{F_{n+1}}\right\rfloor F_{n+1}\right)$$
$$gcd\left(F_{n+1},F_n\right)$$

10. <u>קבעו האם המערכת הבאה פתירה:</u>

$$\begin{array}{rc} 3^9x\equiv 15(48) & 1\\ 47x\equiv 20(3) & 2\\ 24\cdot 2\cdot 21\cdot x\equiv 14(77) & 3\end{array}$$

(א) <u>משוואה 1:</u>

$$3^9x\equiv 15\,(48)$$
$$3^8x\equiv 5(16)$$
$$\varphi(16)=8$$
$$x=1x\equiv 3^{\varphi(16)}x\equiv 5(16)$$

(ב) <u>משוואה 2:</u>

$$47x\equiv 20(3)$$
$$2x+45x\equiv 20(3)$$
$$2x\equiv 20(3)$$
$$x\equiv 10(3)$$

(ג) <u>משוואה 3 :</u>

$$24\cdot 2\cdot 21\cdot x\equiv 14(77)$$
$$24\cdot 2\cdot 3x\equiv 2(11)$$
$$try1$$
$$24\cdot 3x\equiv 1(11)$$
$$6\cdot\underbrace{4\cdot 3}_{12}\equiv 1(11)$$
$$try2-\text{cancel division by 2}$$
$$\underbrace{6\cdot 2}_{12}\cdot\underbrace{4\cdot 3}_{12}x\equiv 2(11)$$
$$x\equiv 2(11)$$

11. <u>בעיית הפעילויות - האלגוריתם מתרגיל 3</u>

<u>טענה 1 :</u> תהי a הפעילות עם זמן הסיום הקטן ביותר ב A . אז קיים פתרון אופטימלי שמכיל את A

<u>טענה 2 :</u> תהי P פתרון אופטימלי עבור מופע A כך שפעולות $k \in P$ אז $p\backslash\{k\}$ מהווה פתרון אופטימלי עבור $A\backslash\{S \in A : b \cap k \neq \phi\}$

12. תחת ההנחה שהטענות 1,2 נכונות נראה שהאלגוריתם מחזיר פתרון אופטימלי

<u>הוכחה: באינדוקציה על גודל הקבוצה A</u>

- עבור $A = \phi$, הטענה נכונה
- נניח כי הטענה נכונה עבור $|A| \leq n$ נשקול קבוצה A הגדול $n+1$
- תהי $a \in A$ פעילות ב A עם זמן סיום קטן ביותר
- ולפי טענה 1 קיים פתרון אופטימלי P עובר A כך ש $a \in P$
- היות ו $|A\backslash\{b \in A : b \cap a \neq \phi\}| < |A|$ שכן a הורדה.
- $\varphi(A\backslash\{b \in A : b \cap a \neq \phi\})$ אזי לפי הנחת האינדוקציה מחזירה פתרון אופיטמלי Q עבור $A\backslash\{b \in A : b \cap a \neq \phi\}$
- לפי טענה 2 , $P\backslash\{a\}$ פתרון אופטימלי עבור $A\backslash\{b \in A : b \cap a \neq \phi\}$, ולכן: $|Q| = |P\backslash\{a\}|$
- ואם כך $|Q \cup \{a\} = |P|$

(א) <u>הוכחת טענה 2</u>

- נניח בשלילה ש $P\backslash\{k\}$ לא אופטימלי ל $A\backslash\{b \in A : b \cap a \neq \phi\}$
- בפרט נניח שקיים Q פתרון אופטימלי למופע זה כך ש: $|Q| > |P\backslash\{k\}|$ ואז היות ו $Q \cup \{k\}$ חוקית
- ייתקים ש $|Q \cup \{k\}| > |P|$ לפי הנחה בשלילה נקבל סתירה למקסמאליות של P

(ב) <u>הוכחת טענה 1</u>

- כמו שהוכחנו בכיתה ללא S_i , (פשוט לקחת את הפעילות הראשונה)

נספח - הגדרות ומשפטים

הגדרות

GCD + מספרים ראשוניים

3.0.12 **אם** a **ו** b **זוג שלמים שלמים נרשום** $a|b$ **לציין ש** a **מחלק את** b **. כלומר ישנו** $k \in \mathbb{Z}$ **כך ש** $b = a \cdot k$ **.**

3.0.13 **יהיו** $a, b \in \mathbb{Z}$ **,** $0 < a, b$ **המחלק המשותף הגדול ביותר של** a **ו** b **נקרא ה** gcd **של** a **ו-** b **:** $greatest - common - divisor$ **ונסמנו ב** (a, b) **וכמובן שניתן לרשום** (b, a) **.**

3.0.14 **הגדרה (אלטרנטיבית ל** gcd**): יהיו** a **ו** b **שלמים, נסמן ב** (a, b) **מספר שמקיים:**

1. אם $(a, b)\,|a$ וגם $(a, b)\,|b$
2. לכל c שלם כך ש $c|a$ וגם $c|b$ מתקיים $c|(a, b)$

3.0.15 **עבור** $a, b \in \mathbb{Z}$ **נגדיר את הקבוצה :** $L(a, b) := \{ma + nb : \ m, n \in \mathbb{Z}\}$

3.0.16 **שני שלמים** a **ו** b **יקראו זרים אם** $(a, b) = 1$

קונגואנציות

3.0.17 **יהי** $m \in \mathbb{Z}^+$ **והיו** $a, b \in \mathbb{Z}$ **, נאמר ש** a **קונוגוראנטי ל** b **מודולו** m **ונרשום** $a \equiv b\,(\mod n)$ **או** $a \equiv b(m)$

3.0.18 **יחס דו-מקומי שהינו רפלקסיבי, סימטרי, טרנזיטיבי נקרא יחס שקילות**

3.0.19 **עבור** $m \in \mathbb{Z}^+$ **נגדיר** $R_m := \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : a \equiv b(m)\}$

3.0.20 **יהי** $m \in \mathbb{Z}^+$ **קבוצה** $x \subseteq \mathbb{Z}$ **תיקרא מערכת שאריות שלמה עבור** m **(או מודלו** m**) אם** $\forall y \in \mathbb{Z}\ \exists! x \in X : \ y \equiv x(m)$ **= לכל** $y \in \mathbb{Z}$ **קיים** $x \in X$ **יחיד כך ש** $y \equiv x\,(mod\ m)$

3.0.21 **יהי** $x \in \mathbb{Z}$ **ויהיה** $m \in \mathbb{Z}^+$ **נסמן ב** $[x]_m$ **את מחלקת השקילות של** $R_{\equiv m}$ **שמכילה את** x

3.0.22 **יהיו** $m \in \mathbb{Z}^+$ **,** $a \in \mathbb{Z}$ **כך ש** $gcd(a, m) = 1$ a **הינו הופכי מודולארי ל** a **מודלו** m **אם** $a \cdot \widetilde{a} = 1(m)$

במילים אחרות: $[a]_m \overset{\text{mod'}}{\cdot} [\tilde{a}]_m = 1$

3.0.23 **יהיו** $m \in \mathbb{Z}^+$ **,** $a \in Z$ **כך ש:** $gcd(a, m) = 1$ **נאמר ש** a **הופכי לעצמו מודולו** m **אם** $a^2 = 1(m)$

3.0.24 **מספר** n **פריק יקרא פסואדו-ראשוני מבסיס** b **אם** $b^n \equiv b(n)$

3.0.25 **הגדרה: מספר פריק** n **כך ש** $b^{n-1} \equiv 1(n)$ **לכל** $b \in \mathbb{Z}$ **כך ש :** $gcd(b, n) = 1$ **נקרא מספר** $Car - Michael$ **קרמייקל.**

3.0.26 **<u>הגדרה</u>: יהי** $n \in \mathbb{Z}^+$ **. נרשום** $\varphi(n)$ **בתור כמות המספרים הטבעיים הקטנים מ** n **שזרים אליו כלומר**

$\varphi(n) = |\{k \in [n] : \ gcd(k, n) = 1\}|$(פונקציה כפלית)

3.0.27 **הגדרה: יהי** $n \in \mathbb{Z}^+$ **, מהי** $A \subseteq \mathbb{Z}$ **כך ש** $|A| = \varphi(n)$ **כך שזו מקיימת:**

1. כל $a \in A$: $gcd(a, n) = 1$
2. כל איברי A אינם קונגוראנטים אחד לשני מודלו n , אזי זו תקרא **מערכת שאריות מצומצת** מודלו n

הגדרה: המכפלה המשותפת הקטנה ביותר של שני מספרי שלמים השונים מאפס a ו b , המסומנת ב $lcm\left(a,b\right)$ הינה lcm השלם החיובי m המקיים את התנאים הבאים:

1. $a|m$ וגם $b|m$
2. אם $a|l$ וגם $b|l$ אז $m \leq l$

משפטים

מבוא

- משפט החלוקה: יהיו a ו b שלמים גדולים מאפס. אז קיימים זוג מספרים r ו q ייחודים כך ש $0 \leq r \leq b$ ומתקיים $a = qb + r$
- אינדוקציה חזקה $\iff$ אינדוקציה חלשה $\iff WOP$
- יהי $a, b \in \mathbb{Z}$ אז קיימים זוג מספרים q ו r יחודים כך ש: $a = q \cdot b + r$ וגם $0 \leq r < b$

GCD

- משפט $bezout$: אם $a, b \in \mathbb{Z}$ אז $(a, b) \in L(a, b) \cap \mathbb{N}$. ובפרט מינימלי בקבוצה זו
- אם $a|c$ ו $b|c$ וגם (a, b) אזי $ab|c$
- אם $a|bc$ ו $(a, b) = 1$ אזי $a|c$:
- כל שלם אם $n > 1$ ניתן להביע אותו באופן ייחודי **כמכפלה של ראשוניים** כך ש: $n = p_1^{a_1} \cdot p_2^{a_2} \cdot, ..., p_n^{a_k}$
  כך ש: $p_1 < p_2 < ..... < p_n$ ובנוסף $a_i \geq 1$ לכל $i \in [k]$
- לכל $n > 1$ שלם קיים מחלק ראשוני
- לכל $n > 1$ שלם ופריק יש מחלק ראשוני $\geq \sqrt{n}$
- אם p ראשוני ובנוסף $p|ab$ אזי $p|a$ או $p|b$
- יהי p ראשוני ויהיו $a_1, ..., a_k$ שלמים כך ש $p|a_1 \cdot .... \cdot a_n$ אז קיים $j \in [n]$ כך ש $p|a_j$
- כל $n > 1$ ניתן להביעו כמכפלה של ראשוניים באופן יחיד עד כדי סדר
- יהיו $a, b, c \in \mathbb{Z}$, $ax + by = c$ פתירה $\iff gcd(a, b)|c$
- אלגוריתם אקולידס לחישוב gcd:
  קלט: $a \geq b \geq 0$ פלט: $gcd(a, b)$

```
Euclid(a,b):
    if b=0
        return a
    else
        return Euclid(b,a mod b)
```

- לכל $a \geq b \geq 0$ שלמים $Euclid(a, b) = gcd(a, b)$ (הרצת האלגוריתם תחזיר את הgcd)
  - טענה: לכל $2 \leq i \in \mathbb{Z}$ מתקיים $x_i \leq b - (i - 1)$
- נרצה להוכיח $Euclid(a, b) = gcd(a, b)$
- יהיו a, b, c אז $gcd(a, b) = gcd(a + bc, b)$
- יהי $a \geq b \geq 1$ אז $gcd(a, b) = (b, a \mod b)$

מספרים ראשוניים

- יש ∞ ראשוניים בעולם
- לכל $n \geq$: $p_n \leq 2^{2^n}$
- לכל $n \geq 2$: $p_n < 2^n$
- משפט $bertrand$: לכל $n \geq 2$ ישנו ראשוני (לפחות אחד) באינטרוול הפתוח $(n, 2n)$
- משפט $Dirichlet$: $gcd(a,b) = 1$ אז בסדרה $an + b$ יש ∞ ראשוניים.
- יש ∞ ראשוניים מהצורה $4n + 3$
- $\{4n - 1 : n \in \mathbb{Z}\} = \{4n + 3 : n \in \mathbb{Z}\}$
- מספר שהינו מכפלה של מספרים מהצורה $4n + 1$ הינו $4n + 1$ בעצמו

קונגראנציות

- $a \equiv b(\mod m) \iff \exists k \in \mathbb{Z}\ a = b + km$
- ל a ול b אותה שארית אחרי חלוקה ב m $\iff a = b(m)$

  כלומר: $a = km + \boldsymbol{r}$, $b = lm + \boldsymbol{r} \iff a = b(m)$

  בלוגיקה היינו מנסחים: $R_m := \{(a,b) \in \mathbb{Z} \times \mathbb{Z} : a \equiv b(m)\}$

  - היחס R_m, הינו יחס שקילות.

- יהיה $m \in \mathbb{Z}^+$ ויהיו $a, b, c \in \mathbb{Z}$ וידוע ש $a \equiv b\,(m)$, אזי:

  1. $a + c = b + c\,(m)$
  2. $a - c \equiv b - c(m)$
  3. $ac = bc(m)$

- משפט - אריטמתטיקה מודלרית: יהי $m \in \mathbb{Z}^+$ ויהיו $a, b, c, , d \in \mathbb{Z}$ כך ש $a = b(m)$ וגם $c \equiv d(m)$

  1. $a + c \equiv b + d(m)$
  2. $a - c \equiv b - d(m)$
  3. $ac \equiv bd(m)$

- משפט (חלוקה מודולרית): יהי $m \in \mathbb{Z}^+$ $a, b, c \in \mathbb{Z}$

$$ac \equiv bc(m) \iff a \equiv b\left(\frac{m}{gcd(c,m)}\right)$$

- <u>למה:</u> יהיו: $\left\{\begin{matrix} x_1 = x_0 + \left(\frac{m}{d}\right) t_1 \\ x_2 = x_0 + \left(\frac{m}{d}\right)_{t_2} \end{matrix}\right\}$, זוג פתרונות שלמים, אזי

$$x \equiv x_2(m) \iff t_1 \equiv t_2(d)$$

- יהי $m \in \mathbb{Z}^+$, $a, b \in \mathbb{Z}$

  1. המשוואה $a \equiv b(m)$ פתירה אס"ם $gcd\,(a,b)\,|b$

2. אם פתירה אז יש לה $gcd(a,m)$ של פתרונות מודולו m שאינם קונגרואנטים אחד לשני

- יהי p ראשוני והי $a \in \mathbb{Z}$ כך ש $gcd(a,p)=1$ אז a הופכי לעצמו מודולו p $\iff$ $a=1(p)$ אזי $a \equiv -1(p) \equiv p-1(p)$

- **משפט השאריות הסיני:** יהיו $n_1,n_2,...,n_r$ מספרים שלמים חיוביים שזרים בזוגות אזי למערכת $\begin{Bmatrix} x \equiv a_1(n_1) \\ x \equiv a_2(n_2) \\ \vdots \\ x \equiv a_r(n_r) \end{Bmatrix}$ קיים פתרון יחיד מודלו $\prod_{i=1}^{r} n_i$

- <u>משפט $(wilson)$</u> : יהיה p ראשוני אזי $(p-1)! \equiv -1(p)$

- <u>משפט (הפוך $wilson$</u> : אם $(n-1)! \equiv -1(n)$ אז n ראשוני.

- משפט פרמה הקטן: יהי p ראשוני ויהי $gcd(a,p)=1$ אז $a^{p-1} \equiv 1(p)$
  - בניסוח שקול: : יהי p ראשוני, ויהיה $a \in \mathbb{Z}$ אזי $a^p \equiv a(p)$

- יהיה $n=q_1 q_2 \cdot ..... \cdot q_k$ כאשר $\{q_i\}_{i=1}^{k}$ ראשוניים, ובנוסף $\forall j \in [k]$ אם $q_j-1|n-1$ אז n הינו $Car-Michael$

- משפט $Euiler$: עבור $n \in \mathbb{Z}^+$ ויהי a כך ש $gcd(a,n)=1$ אז $a^{\varphi(n)} \equiv 1(n)$

- $\varphi(n)=n=1$ $\iff$ n ראשוני

- משפט: יהי $n \in \mathbb{Z}^+$ ותהי $\{r_1,r_2,...,r_{\varphi(n)}\}$ מערכת שאריות מצומצת מודלו n . והיה $a \in \mathbb{Z}$ כך ש $gcd(a,n)=1$, אזי $\{ar_1,ar_2,...,a_{r\varphi(n)}\}$ הינה גם מערכת שאריות מצומצמת מדולו n

- טענה: φ הינה כפלית

RSA

- בעצם אנחנו רוצים:

$$P_A(S_A(m)=m=S_A\left(P_A(m)\right)$$

- האלגוריתם:
  - פלט S,P
    1. מצא שני ראשוניים p ו q "<u>ענקיים</u>"
    2. קבע $n:=p \cdot q$
    3. מצא מספר אי־זוגי e כך שמתקיים $gcd\left(e,\varphi(n)\right)=1$
    4. קבע d להיות ההופכי של e במודלו $\varphi(n)$
    5. פלט: מפתח ציבורי:= $\langle e,n \rangle$. מפתח פרטי:= $\langle d,n \rangle$
  - מהם אם כך P ו S ? $\forall m_{\text{a letter}} \in \left\{[0]_n,[1]_n,...[n-1]_n\right\}$ נגדיר $P(m)=m^e(n)$, $S(m)=m^d(n)$

- טענה: לכל $m \in [0,n-1]$ מתקיים ש: $P_A(S_A(m)=m=S_A\left(P_A(m)\right)$
  - למה 1: מתקיים ש: $P_A(S_A(m)=\left(P_A(m)\right)$:
  - למה 2 : $m^{ed} \equiv [m]_n$, $\forall m \in [0,n-1]$