לקראת המבחן

0.1 מבוא + משפט החלוקה + GCD

קבוצת הטבעיים $\mathbb{N}$:

1. $1 \in \mathbb{N}$
2. אם $n \in \mathbb{N}$ אז גם $n+1 \in \mathbb{N}$

0.1.1 אקסיומת WOP : לכל תת קבוצה לא ריקה של $\mathbb{N}$ יש איבר מינמלי

0.1.2 אינדוקציה חלשה:

תהי $S \subseteq \mathbb{N}$ המקיימת:

$I.1$ $1 \in S$

$I.2$ אם $k \in S$ אז $k+1 \in S$

אז $S = \mathbb{N}$

<u>הוכחה ־ wop $\Leftarrow$ חלשה:</u>

- נניח בשלילה $S \neq \mathbb{N}$, ונגדיר $T := \mathbb{N} \backslash S$(המשלימה ל S)
- לפי wop ישנו איבר מינימלי ב T , ונוכל לסמנו ב a.
- נשים לב ש $1 \in S$ ולכן $a > 1$
- מכאן נובע שעבור $a-1 \in \mathbb{N}$ מתקיים ש: $a-1 \notin T$
- ומהגדרת T נובע ש: $a-1 \in S$, אבל מ $I.2$ גם $a-1+1 = a \in S$
- בסתירה לכך ש $a \in T \equiv \mathbb{N} \cap \bar{S}$

0.1.3 אינדוקציה חזקה:

תהי $S \subseteq \mathbb{N}$ תת קבוצה המקיימת:

$S.1$ $1 \in S$

$S.2$ אם $\{0,1,2...n\} \subseteq S$ אז $n+1 \in S$

אז $S = \mathbb{N}$

<u>הוכחה ־ חלשה $\Leftarrow$ חזקה:</u>

תהי $S \subseteq \mathbb{N}$ המקיימת את את תנאי אינדוקציה החלשה:

- נתון: $I.1$ בו $1 \in S$ <u>צ"ל</u> $S.2$ ־ $1 \in S$, וזה מתקיים מיידית.
- נתון : $I.2$ אם $k \in S$ אז $k+1 \in S$ <u>צ"ל</u>: אם $\{0,1,2...n\} \subseteq S$ אז $n+1 \in S$, גם מתקיים מיידית בעבור $n=k$

<u>הוכחה ־ חזקה $\Leftarrow$ WOP :</u>

- נניח בשלילה שקיימת קבוצה $S \subseteq \mathbb{N}$ שאין לה איבר מינימלי.
- תהיה $T := \mathbb{N} \backslash S$. כלומר הקבוצה המשלימה של S.
- נתבונן ב 1 : $1 \in \mathbb{N}$ מינימלי, והנחנו בשלילה של S אין איבר מינימלי ולכן $1 \notin S$ $\Leftarrow$ $1 \in T$ $\Leftarrow$ T מקיימת את $S.1$

- נניח אם כן, ש $\{1,2....,n\} \subseteq T$, נרצה להראות ש $n+1 \in T$ $(S.2)$
  - נניח בשלילה ש $n+1 \in S$.
  - היותו $1,2,...,n \notin S$ נובע ש $n+1 \in S$ מינימלי שם, וזו סתירה להגדרת S ,
  - לכן $n+1 \in T$
- לכן $T = \mathbb{N}$
- ולכן $S \neq \phi$, (כלומר קבוצה ללא איבר מינמלי היא קבוצה ריקה $\Longleftrightarrow$ אין כזו)

0.1.4 הראנו $WOP \Leftarrow$ חלשה $\Leftarrow$ חזקה $\Leftarrow WOP$, ומכאן ששקולים.

0.1.5 בונוס : הוכחה - חזקה $\Leftarrow$ חלשה:

תהיה $S \subseteq \mathbb{N}$, המקיימת $1 \in S$, וגם שאם $\{0,1,2...n\} \subseteq S$ אז $n+1 \in S$. צ"ל ש $S = \mathbb{N}$.

- נגדיר $Q = \{n \in \mathbb{N} : k \in S \ \forall k < n\} \cup \{1\}$, נראה ש $Q = \mathbb{N}$ (ע"י אינדוקציה חלשה):
  - מהגדרת Q , $1 \in Q$, ולכן $I.1$ מתקיים.
  - כעת צ"ל את $I.2$: אם $n \in Q$ אז $n+1 \in Q$ (לשים לב למעבר בין Q ל S וחזרה)
    * יהיה $n \in Q$ מהגדרת Q , נובע ש: $\{1,2...,n-1\} \subseteq S$
    * מנתון ש $S.2$ מתקיים נובע שגם $n \in S$, ולכן $\{1,2...,n\} \subseteq S$
    * לכן מהגדרת Q גם $n+1 \in Q$
- כעת נרצה להראות ש $S = \mathbb{N}$, נראה זאת ע"י הכלה דו-כיוונית
  - נראה ש $\mathbb{N} \subseteq S$:
    * יהי $n \in \mathbb{N}$ הראנו ש $Q = \mathbb{N}$, ולכן $n \in Q$
    * מהגדרת Q יתקיים ש: $\{1,2,...,n-1\} \subseteq S$
    * אז מכך ש $S.2/I.2$ נובע גם ש $n \in S$
  - ולכן $\mathbb{N} \subseteq S$
  - נתון $S \subseteq \mathbb{N}$
- ובסה"כ $S = \mathbb{N}$, כנדרש.

0.1.6 משפט החלוקה: יהי $a,b \in \mathbb{Z}$ כך ש $b > 0$ אז קיימים זוג מספרים r,q יחודיים כך ש: $a = qb + r$ וגם $0 \leq r < b$

<u>קיום:</u>

- נגדיר $s = \{a - bk : \ k \in \mathbb{Z}, a - bk \geq 0\}$ (קבוצת השאריות)
- נראה ש: $S \neq \phi$
  - נציב $k = -|a| - 1$, מכך ש $b > 0$ נקבל ש:

$$a - (|a| - 1)\, b = a + |a|\, b + b \geq a + |a| + 1 \geq 0$$

- לכן ע"פ wop יש ל S איבר מינימלי, נסמנו ב r שעבורו $r = a - bq$ עם $q \in \mathbb{Z}$, ובכך הראנו r,q קיימים
- נראה שגם תנאי 2 מתקיים , כלומר $0 \leq r < b$.
- מהגדרת S , $0 \leq r$, נותר לוודא שאכן $r < b$:

- נניח בשלילה ש $r \geq b$, ונזכר ש $b > 0$, יתקיים ש:

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

- ולכן גם $r - b \in S$ וברור ש $r - b < r$, וזו סתירה למינימליות של r

<u>יחודיות:</u>

- נניח בשלילה שאינם יחידים, כלומר $\begin{array}{ll} a = bq_1 + r_1 & 0 \leq r_1 < b \\ a = bq_2 + r_2 & 0 \leq r_2 < b \end{array}$

- היות ו $r_1, r_2 \in [0, b-1]$ נובע ש:

$$-b < r_2 - r_1 < b$$

- מההנחה בשלילה נובע ש:

$$\begin{gathered} bq_1 + r_1 = bq_2 + r_2 \\ \Updownarrow \\ b\left(q_1 - q_2\right) = r_2 - r_1 \\ \Updownarrow \\ b | r_2 - r_1 \end{gathered}$$

- לכן אם $b | r_2 - r_1$ וגם $-b < r_2 - r_1 < b$ יכול להתקיים רק ש : $r_2 - r_1 = 0 \iff r_2 = r_1$, סתירה לכך שהם שונים

0.1.7 משפט $bezout$: $gcd(a,b) \in \{ma + nb : \ n, m \in \mathbb{Z}\}$ ומינימלי

<u>הוכחה:</u>

- נסמן $L(a,b) \cap \mathbb{Z}^+ = \{ma + nb : \ n, m \in \mathbb{Z}\}$
- נבחר $m = a, b = n$ יתקיים ש: $ma + bn = a^2 + b^2 \in \mathbb{Z}$, ומכאן ש $L(a,b) \cap \mathbb{Z}^+$ לא ריקה.
- לכן ע"פ wop יש לה איבר מינימלי, נסמנו ב d , כלומר $d \in L(a,b) \cap \mathbb{Z}^+$
- כלומר קיימים $m, n \in \mathbb{Z}$ כך ש: $d = ma + nb$
- <u>צ"ל:</u>
  - $d|a$ וגם $d|b$
  - $d = Max\left\{D(a) \cap D(b)\right\}$
- <u>$d|a$ (נראה בעזרת משפט החלוקה בהצבת a, d):</u>
  - על פי משפט החלוקה מתקיים ש: $a = qd + r$ כך ש: $0 \leq r < d$
  - אם $r = 0$ אז $q \in \mathbb{Z}$ ויתקיים ש: $a = qd \iff d|a$
  - לכן נניח בשלילה ש: $r > 0$, ויתקיים :

$$0 < \boldsymbol{r} = a - qd = a - q\left(ma + nb\right) = a - qma - qnb = \left(1 - qm\right)a - \left(qn\right)b$$

  - לכן: $r = \left(1 - qm\right)a - \left(qn\right)b \in\in L(a,b) \cap \mathbb{Z}^+$
  - והרי: $r < d$, וזו סתירה למינימליות של d

- $d|b$: באופן סימטרי
- $d = Max\{D(a) \cap D(b)\}$:
  - מספיק להראות שלכל $c \in \{D(a) \cap D(b)\}$, $c|d$
  - יהי c שכזה, אז:

$$\frac{d}{c} = \frac{ma+nb}{c} = m\left(\frac{a}{c}\right) + n\left(\frac{b}{c}\right)$$

  - והרי $c|b$ וגם $c|a$ ולכן שנים ב $\mathbb{Z}$, והביטוי מוגדר היטב

0.1.8 אם $a|c$ **ו** $b|c$ **וגם** $gcd(a,b) = 1$ **אז** $ab|c$

0.1.9 אם $a|bc$ **ו** $gcd(a,b) = 1$ **אז** $a|c$

0.1.10 יהי p **ראשוני ויהי** $a_1, ...a_k$ **מספרים שלמים כך ש:** $p|a_1 \cdot ....a_k$ **אז קיים** $j \in [k]$ **כך ש:** $p|a_j$

הוכחה:

בסיס:

$n = 1$, טרויאלי

$n = 2$ נובע מ $0.0.9$

צעד: נניח שהטענה נכונה ל n ונוכיח בעבור $n+1$. כלומר נניח ש $p|a_1....a_na_{n+1}$ צ"ל שקיים $j \in [n+1]$ כך ש $p|a_j$

- יהיה $n' = a_1....a_na_{n+1}$ אם $p|a_1....a_n$ אז מהנחת האינדוקציה סיימנו.
- אחרת, נובע ש: $gcd(p, a_1....a_n) = 1$, ולכן על פי משפט $0.0.9$, $p|a_{n+1}$
- לכן $j = n+1$, וסיימנו.

0.1.11 המשפט היסודי של הארימתטיקה: כל שלם אם $1 < n$ **ניתן להביע באופן יחודי כמכפלה של ראשוניים:** $n = p_1^{a_1} \cdot p_2^{a_2} \cdot ...p_k^{a_k}$ **כך ש:** $p_1 < p_2 < .... < p_k$

קיום:

- נניח בשלילה כי כי ישנם מספרים חיוביים טבעיים שלא יכולים להירשם בצורה שכזו
- יהיה n מינימלי שכזה.
- אם נניח ש n ראשוני, אז הוא מכפלה של עצמו, וקבילנו סתירה, וסיימנו.
- לכן נניח ש n פריק, וניתן להביעו כי $n = ab$ עבור $2 \leq a, b < n$
- נתבונן ב a : $a < 2$, ו n הוא המינימלי שלא יכול להרשם כמכפלה של ראשוניים
- ולכן קיים $p \in \mathbb{Z}^+$ שבעבורו $p|a$ והרי $a|n$ לכן מטרנזיטיביות $p|n$, וזו סתירה

יחודיות:

- נניח בשלילה שקיימים פירוקים שונים, הנותנים $n = \prod_{i=1}^{k} p_i^{a_i} = \prod_{j=1}^{l} q_j^{b_j}$
- לכן נרשום: $\prod_{i=1}^{k} p_i^{a_i} = \prod_{j=1}^{l} q_j^{b_j}$, אם יש מספרים זהים נצמצם, ולכן ניתן להניח שבביטוי הנ"ל כל המספרים **שונים**
- יתקיים ש: $p_1 \prod_{i=2}^{k} p_i^{a_i} = \prod_{j=1}^{l} q_j^{b_j} \Leftarrow p_1|q_1^{b_1}....q_l^{b_l}$
- ממשפט קודם ישנו $j \in [l]$ כך ש $p_1 = q_j$, בסתירה לכך שאין גורמים משותפים ביין הייצוגים

0.1.12 לכל $1<n$ שלם ופריק יש מחלק ראשוני $\leq \sqrt{n}$

- יהי $n=ab$ כך ש $2\leq a,b<n$
- ניתן להניח שלפחות אחד מ a,b קטן מ $\sqrt{n}$, אחרת $ab>n$
- בה"כ נניח שזה a , כלומר $a\leq\sqrt{n}$
- ע"פ הוכחת קיום למשפט היסודי לאריתמטיקה ל a יש מחלק ראשוני, כנדרש.

0.1.13 יהי $a,b,c\in\mathbb{Z}$ המשוואה $ax+by=c$ פתירה $\iff gcd(a,b)|c$

הוכחה - גרירה דו־כיוונית:

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

- נניח ש x_0,y_0 מהווים פתרון למשוואה דהיינו $ax_0+by_0=c$
- לכן ישנם $k,l\in\mathbb{Z}$ כך ש: $gcd(a,b)\cdot lx_0+gcd(a,b)\cdot ky_0=c \iff lx_0+ky_0=\frac{c}{gcd(a,b)}$
- צד שמאל הוא ביטוי ב $\mathbb{Z}$,ו לכן גם $\frac{c}{gcd(a,b)}\in\mathbb{Z}$ כנדרש.

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

- נניח כי $gcd(a,b)|c$ לכן ישנו $l\in\mathbb{Z}$ שבעבורו:

$$gcd(a,b)|c \iff gcd(a,b)\cdot l=c \overset{bezout}{\iff} c=(am+bn)\cdot l=lam+lbn$$

- נסמן $lm=x_0$, ו $bn=y_0$, ונקבל את הדרוש

0.1.14 יהיו a,b,c אם $gcd(a,b)=gcd(a+bc,b)$

נזכר שהגדרנו את gcd כמקסימלי מבין קבוצת המחלקים, לכן אם נראה:

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

כלומר שקבוצת המחלקים זהות, סיימנו

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

- יהי $e\in D(a)\cap D(b)$ אז $e|a$ וגם $e|b$ ובפרט $e|bc$
- וממפשט מתקיים גם $e|a+bc \Leftarrow e\in D(a+cb)\cap D(b)$

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

- יהי $f\in D(a+cb)\cap D(b)$ אז $f|b$ וגם $f|a+bc$ לכן $f|a+bc-bc$
- כעת: $f|a+bc-bc \iff f|a$, לכן $f\in D(a)\cap D(b)$, כנדרש.

יהי $a\geq b>1$ אז $gcd(a,b)=gcd(b,a \mod b)$

הוכחה:

- (ממשפט החלוקה) לכל a מתקיים ש: $a=\underbrace{b\left\lfloor\frac{a}{b}\right\rfloor}_{bq}+\underbrace{a \mod b}_{r} \iff a \mod b=a-b\left\lfloor\frac{a}{b}\right\rfloor$
- ממשפט קודם:

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

0.1.15 אלגוריתם של אוקלידס

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

0.1.16 לכל $a \geq b > 0$ שלמים $Euclid(a,b) = gcd(a,b)$

למה: תהי הסידרה $\left\{\begin{array}{c} x_1 = b \\ x_2 = a \mod b \\ x_{i+1} = x_{i-1} \mod x_i \end{array}\right\}$ **לכל** $2 \leq i \in \mathbb{Z}$ **מתקיים ש:** $x_i \leq b - (i-1)$

<u>הוכחה - באינדוקציה:</u>

<u>בסיס:</u>

- עבור $i = 2$ מתקיים ש: $x_2 = a \mod b \leq b - 1 = b - (2-1)$

<u>צעד:</u> נניח שטענה זו נכונה בעבור i ונוכיח ל $i+1$

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

<u>הוכחה</u> <u>$(Euclid(a,b) = gcd(a,b))$</u>

- מהלמה לכל $2 \leq i \in \mathbb{Z}$: $x_{b+1} \leq b - (b+1-1) \leq 0$
- מצד שני, מהגדרת הסידרה לכל $x_i \geq 0$ בפרט $x_{b+1} \geq 0$
- בסה"כ : $0 \leq x_{b+1} \leq 0 \Leftarrow x_{b+1} = 0 \Leftarrow$ אלגוריתם אקולידס מגיע לכדי סיום.

(לכן אם נוכיח ש $gcd(a,b) = gcd(b, a \mod b)$ סיימנו, ראה לעיל)

0.1.17 יש ∞ ראשוניים בעולם

- נניח בשלילה שישנו מספר סופי של ראשוניים $p_1, ...p_n$, כאשר p_n הראשוני המקסימלי
- נגדיר מספר חדש $Q = p_1 \cdot .... \cdot p_n + 1$
- ברור ש $Q > p_1 \cdot .... \cdot p_n > p_n$, ולכן אם Q ראשוני, הגענו לסתירה וסיימנו.
- לכן נניח ש Q פריק, לכן קיים p ראשוני כלשהו כך ש $p \leq p_n$ המקיים:
  - $p|Q$
  - וברור שגם $p|p_1 \cdot ... \cdot p_n$
  - לכן ממשפט $p|Q - p_1 \cdot .... \cdot p_n = 1$
  - לכן $p|1 \iff p \leq 1$ סתירה לכך ש p ראשוני.
- לכן ישנם ∞ ראשוניים כנדרש

0.1.18 מסקנה: $p_{n+1} \leq Q = p_1 \cdot .... \cdot p_n + 1$

- אם Q ראשוני אז נבחר $p_{n+1} = Q$ ויתקיים ש: $Q|Q$
- אם Q פריק, אז בהוכחה קודמת הראינו שאם $p < p_n$ $\iff$ $p = 1$ $\iff$ p אינו ראשוני
- לכן ישנו $p_{n+1} > p_n$ כך ש: $p_{n+1}|Q$ ולכן $p_{n+1} < Q$

0.1.19 משפט: לכל $n \in \mathbb{N}$ **:** $p_n \leq 2^{2^n}$

נראה באינדוקציה:

<u>בסיס:</u> עבור

$$\begin{array}{ll} \underline{n=1} & p_1 = 2 \leq 2^{2^1} \\ \underline{n=2} & p_2 = 3 \leq 2^{2^2} \end{array}$$

<u>צעד:</u> נניח ל $k \leq n$ נוכיח ל $n+1$:

$$p_{n+1} \leq p_1 ... p_n + 1 \leq 2^{2^1} 2^{2^2} ... 2^{2^n + 1} = 2^{\sum\limits_{k=1}^{n} 2^k} + 1 \leq 2^{2^{n+1}-1} + 1 \leq 2 \cdot 2^{2^{n+1}-1} = 2^{2^{n+1}}$$

0.1.20 משפט ברטרנד: לכל $n \geq 2$ **ישנו ראשוני ־ לפחות אחד ־ בקטע** $(2, 2n)$ **(ללא הוכחה)**

0.1.21 מסקנה: לכל $n \geq 2$ $p_n < 2^n$

<u>הוכחה ־ באינדוקציה:</u>

<u>בסיס:</u>

$$\begin{array}{ll} \underline{n=1} & p_1 = 2 < 2^2 \\ \underline{n=2} & p_2 = 3 < 2^3 \end{array}$$

<u>צעד:</u> נניח ל n נוכיח ל $n+1$

- ע"פ ברטנרד בקטע $\left(2^n, 2^{n+1}\right)$ ישנו q ראשוני כך ש:

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

- ברור ש $p_n < p_{n+1}$ ומהנחת האינדוקציה:

$$p_n < 2^n < q < 2^{n+1} \Rightarrow p_{n+1} < 2^{n+1}$$

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

<u>הוכחה</u> ־ הכלה דו־כיוונית:

- <u>כיוון ראשון ־ $\{4n+3 : \ n \in \mathbb{Z}\} \subseteq \{4n-1 : \ n \in \mathbb{Z}\}$:</u>
  - יהי $x \in \{4n+3 : \ n \in \mathbb{Z}\}$ אז קיים n' כך ש:

$$x = 4n' + 3 = 4n' + 4 - 4 + 3 = 4(n'+1) - 1$$

  - לכן אם נסמן $m' = n' + 1$ נקבל ש:

$$x = 4m' - 1 \in \{4n-1 : \ n \in \mathbb{Z}\}$$

- <u>כיוון שני ־ $\{4n-1 : \ n \in \mathbb{Z}\} \subseteq \{4n+3 : \ n \in \mathbb{Z}\}$:</u>
  - סימטרי

0.1.23 **למה 2 : מכפלת מספרים מהצורה $4n+1$ נשארת בצורה זו**

<u>הוכחה ־</u> אינדוקציה על האיברים המכפלים:

<u>בסיס:</u>

- $n=1$ ־ טריוויאלי
- $n=2$ אז, יהיו $n,m\in\mathbb{Z}$:

$$(4m+1)(4n+1)=...=4(4mn+n+m)+1$$

<u>צעד:</u> נניח ל $k<n$ נוכיח ל n :

$$\prod_{k=1}^{n}(4k+1)=(4n+1)\prod_{k=1}^{n-1}(4k+1)=(4n+1)(4m+1)=\{\text{as n=2}\}$$

0.1.24 **יש ∞ ראשונים מהצורה $4n+3$**

- נניח בשלילה שיש מספר סופי של איברים מהצורה $4n+3$ כלומר $S=\{4n+3\ n\in\mathbb{Z}\}$ סופית
- $3\in S$ ולכן $S\neq\phi$
- נגדיר $Q=4(q_1,....q_n)-1$
- Q אי־זוגי, לכן $2\nmid Q$
- כמו כן $Q>q_n$ ולכן אם Q ראשוני הגענו לסתירה, וסיימנו.
- לכן נניח כי Q פריק $\iff$ יש לו מחלק ראשוני $3\leq q\leq q_n$
  - לכן $q|Q$
  - ולכן $q|4(q_1...q_n)$
  - לכן: $q|4(q_1...q_n)-Q=4(q_1,....q_n)-4(q_1...q_n)+1=1$
  - לכן $q\leq 1$ סתירה לכך ש $q\geq 3$
- על פי למה 2 , $q\neq 4n+1$, והראנו שאינו זוגי, לכן q מהצורה $4n+3$
- על פי למה 1, כיון ש Q מהצורה $4n-1$ הוא שקול לצורה $4n+3$
  - לכן q הוא ראשוני חדש מהצורה $4n+3$ או ש Q עצמו ראשוני חדש מהצורה $4n+3$

0.1.25 **משפט $Dirichlet$: יהיו a,b כך ש $gcd(a,b)=1$ אז בסדרה $an+b$ יש ∞ ראשוניים (ללא הוכחה)**

0.2 קונגראנציות

0.2.1 $a\equiv b(\mod m)\iff\exists k\in\mathbb{Z}\ a=b+km$

- מהגדרה: $a\equiv b(\mod m)\iff m|a-b\iff\exists k\in\mathbb{Z}:\ mk=a-b\iff\exists k\in\mathbb{Z}\ a=b+km$

0.2.2 ל a ו b אותו שארית חלוקה מודולו m $\iff$ $a \equiv b(m)$

נסמן: $a = mk_1 + r, b = mk_2 + r$ צ"ל ש: $a = bk_1 + r, b = bk_2 + r \iff a \equiv b(m)$

$a \equiv b(m) \Rightarrow a = mk_1 + r, b = mk_2 + r$:

- נניח ש $a \equiv b(m)$, ממשפט קודם קיים $k \in \mathbb{Z}$ ש: $a = b + km$
- נפעיל את משפט החלוקה על b, m נקבל שישנו r כך ש: $b = lm + r$,
- לכן $a = lm + r + km = m(l + k) + r$ (ואכן rים זהים)

$a = mk_1 + r, b = mk_2 + r \Rightarrow a \equiv b(m)$:

- נניח ש: $\begin{matrix} a = mk_1 + \boldsymbol{r} \\ b = mk_2 + \boldsymbol{r} \end{matrix}$ צ"ל ש $m|a - b$
- מתקיים ש: $m|a - b = mk_1 + \boldsymbol{r} - mk_2 - \boldsymbol{r} = m(k_1 - k_2)$ ✓

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

0.2.3 R_m הוא יחס שקילות

1. רפלקסיבי: יהיה $a \in \mathbb{Z}$ מתקיים ש: $a - a = 0|m \iff a \equiv a|m$
2. סימטרי: יהיו $a, b \in R_m$ אז $a \equiv b(m) \iff m|a - b \iff m|b - a \iff b \equiv a(m)$
3. טרנזיטיבי: יהיו $a, b \in R_m$ ו $b, c \in R_m$ צ"ל ש $a \equiv c(m)$
   - מנתון $a \equiv b(m) \iff m|a - b$ ו $b \equiv c(m) \iff m|b - c$
   - לכן: $m|(a - b) + (b - c) = a - c \iff a \equiv c(m)$

0.2.4 יהי $m \in \mathbb{Z}^+$. כל קבוצה של m מספירם לא שקולים מדולו m מהווה מערכת שאריות שלמה מודולו m

0.2.5 אריתמטיקה מודלרית יהי $m \in \mathbb{Z}^+$ והיו $a, b, c, d \in \mathbb{Z}$ כך ש $a \equiv b(m)$ וגם $c \equiv d(m)$

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

הוכחה:

- נתון כי ישנם k, l כך ש: $\begin{matrix} a = b + km \\ c = d + lm \end{matrix}$ אז:

$$a + c = b + km + d + lm = b + d + m(k + l) \equiv b + d(m)$$

- נתון כי ישנם k, l כך ש: $\begin{matrix} a = b + km \\ c = d + lm \end{matrix}$ אז:

$$a - c = b + km - d - lm = b - d + m(k - l) \equiv b - d(m)$$

- נתון כי ישנם k, l כך ש: $\begin{matrix} a = b + km \\ c = d + lm \end{matrix}$ אז:
- $ac \equiv bd(m) \iff m|ac - bd$ לכן אם נראה זאת , סיימנו

$$ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d) = ckm + blm = m(kc + bl)$$

0.2.6 חלוקה מודולרית: יהי $m \in \mathbb{Z}^+$ $a,b,c \in \mathbb{Z}$ **אז:** $ac \equiv bc(m) \not\Longleftrightarrow a \equiv b\left(\frac{m}{c}\right)$

למשל:

$$\begin{gathered}14 \equiv 8(6)\\ 7 \cdot \cancel{2} \equiv \cancel{2} \cdot 4(\cancel{2} \cdot 3)\\ 7 \not\equiv 4(3)\end{gathered}$$

0.2.7 חלוקה מודולרית: יהי $m \in \mathbb{Z}^+$ $a,b,c \in \mathbb{Z}$ **אז:** $ac \equiv bc(m) \iff a \equiv b\left(\frac{m}{gcd(c,m)}\right)$

<u>הוכחה:</u>

<u>$ac \equiv bc(m) \Rightarrow a \equiv b\left(\frac{m}{gcd(c,m)}\right)$:</u>

- נניח ש $ac \equiv bc(m) \iff m|ac-bc \iff m|c(a-b)$
- לכן ישנו $k \in \mathbb{Z}$ כך ש: $mk = c(a-b)$
- נגדיר $\begin{Bmatrix} r \cdot gcd(c,m) = c \\ r = \frac{c}{gcd(c,m)} \end{Bmatrix}$ ונגדיר $\begin{Bmatrix} s \cdot gcd(c,m) = m \\ s = \frac{m}{gcd(c,m)} \end{Bmatrix}$ עם $gcd(r,s) = 1$
- נציב: $mk = c(a-b) = s \cdot \cancel{gcd(c,m)} \cdot k = r \cdot \cancel{gcd(c,m)}(a-b)$
- לכן $sk = r(a-b) \iff s|r(a-b)$ נזכר s,r זרים , ולכן $s|a-b \iff a \equiv b(s) \iff a \equiv b\left(\frac{m}{gcd(c,m)}\right)$

<u>$ac \equiv bc(m) \Leftarrow a \equiv b\left(\frac{m}{gcd(c,m)}\right)$:</u>

- סימטרי

0.2.8 מסקנות:

1. אם $gcd(c,m) = 1$ אז $a \equiv b(m) \iff ac \equiv bc(m)$
2. אם $m = p$ ראשוני כך ש $c \nmid m$ אז $a \equiv b(p) \iff ac \equiv bc(p)$

<u>הוכחה:</u> הצבה במשפט

0.2.9 משפט: יהי $m \in \mathbb{Z}^+$, $a,b \in \mathbb{Z}$

1. המשוואה $a \equiv b(m)$ פתירה $\iff$ המשוואה $ax+by=c$ פתירה $\iff gcd(a,m)|b$
2. אם פתירה, כל פתרון יהיה מהצורה $\begin{Bmatrix} x = x_0 + \left(\frac{b}{d}\right)t \\ y = y_0 - \left(\frac{a}{d}\right)t \end{Bmatrix}$, כאשר : $\langle x_0, y_0\rangle$הם פתרון , $d = gcd(a,b)$, ו $t \in \mathbb{Z}$ שרירותיים
3. אם פתירה יש לה $gcd(a,m)$ פתרונות מודולו m שאינם קונגרורנטים אחד לשני

הוכחה:

1. מתקיים ש:

$$a \equiv b(m) \iff ax \equiv b(m) \iff ax = -by + km \iff ax + by = c$$

- ואת השקילות: המשוואה $ax+by=c$ פתירה $\iff gcd(a,m)|b$ הראנו לעיל (לפני אולג' אוקלידס).

2. **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 פתרונות שלמים אז:** $t_1 \equiv t_2(d) \iff x \equiv x_2(m)$

- 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 למשוואה כך ש $x_1 \equiv x_2(m)$
- אז מארימתטיקה וחלוקה מודלארית:

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

- כאשר $d = gcd(m, \frac{m}{d})$ ולכן $\frac{m}{d}|m$ נקבל ש $d = \frac{m}{d}$
- מסקנות:
  - נזדקק לתת ל t , d ערכים על מנת לקבל את כל הפתרונות שאינם שקולים מודולו m
  - הטענה שכל פתרון יראה מהצורה: $\begin{Bmatrix} x = x_0 + \left(\frac{b}{d}\right) t \\ y = y_0 - \left(\frac{a}{d}\right) t \end{Bmatrix}$ נובעת כמקרה פרטי של בחירת t יחיד.
  - <u>על כן אלגוריתם לפתירת משוואה:</u>
    * הפעלת אוליקדס המורחב לקבלת השלילה $\langle d, x_0, y_0 \rangle$ המקיימת $ax_0 + by_0 = d = gcd(a,b)$
    * נכפיל ב c : $cax_0 + cby_0 = dc$
    * נחלק ב d : $a\left(\frac{cx_0}{gcd(a,b)}\right) + b\left(\frac{cy_0}{gcd(a,b)}\right) = a\left(\frac{cx_0}{d}\right) + b\left(\frac{cy_0}{d}\right) = c$

3. נניח שפתירה ולכן:

- נניח כי $d := gcd(a,b)|b$. בנוסף $ax = b - my \iff ax \equiv b(\mod m) \iff a \equiv b(m)$
- מאוקלידס המורחב למשוואה $ax + my = b$ יש פתרונות בשלמים כך ש: $\begin{Bmatrix} x = x_0 + \left(\frac{m}{d}\right) t \\ y = y_0 - \left(\frac{a}{d}\right) t \\ t \in \mathbb{Z} \end{Bmatrix}$
- מהלמה ב 2 , נובע כי צריך לתת d ערכים ל t , לקבלת מספר הפתרונות שאינם שקולים מודולו m

משפט השאריות הסיני

הגדרות:

- יהיו $\begin{matrix} m \in \mathbb{Z}^+ \\ a \in \mathbb{Z} \end{matrix}$ כך ש: $gcd(a,m) = 1$. נאמר ש $\widetilde{a}$ **הופכי מודלארי ל** a **מודולו** m אם $a \cdot \bar{a} = 1$ כלומר $[a]_m \cdot [\widetilde{a}]_m = 1$
- יהיו $\begin{matrix} m \in \mathbb{Z}^+ \\ a \in \mathbb{Z} \end{matrix}$ כך ש: $gcd(a,m) = 1$. נאמר ש a **הופכי לעצמו ל** a **מודולו** m אם $a \cdot a = 1$ כלומר $a^2 = 1(m)$

0.2.10 יהי p **ראשוני ו** $a \in \mathbb{Z}$ **כך ש** $gcd(a,p) = 1$ **אז (** a **הופכי לעצמו מודולו** p**)** $a^2 = 1(p) \iff$

<u>הוכחה:</u>

<u>כיוון ראשון - a הופכי לעצמו מודולו p $\Rightarrow$ $a = 1(p)$ או $a \equiv -1(p) \equiv p - 1(p)$:</u>

- אם $a \equiv \pm 1(p)$ אז $a \cdot a = a^2 \equiv (\pm 1)(\pm 1) \equiv (\pm 1)^2\,(p) \equiv 1(p)$, כנדרש.

<u>כיוון שני - a הופכי לעצמו מודולו p $\Leftarrow$ $a = 1(p)$ או $a \equiv -1(p) \equiv p - 1(p)$</u>

- נניח ש $a^2 \equiv 1(p) \iff p|a^2-1=(a-1)(a+1)$
- לכן:
  - אם $p|(a-1) \iff a \equiv -1(p)$
  - או $p|a+1 \iff a \equiv 1(p)$

0.2.11 משפט וילסון: יהיה p ראשוני אז $(p-1)! \equiv -1(p)$

<u>הוכחה:</u>

- <u>עבור $p=2$</u> נציב: $(2-1)!=1\equiv -1(2)$
- <u>עבור $p>2$:</u>
  - לכל $a\in[p-1]$ יש איבר b הופכי מודלארי ל a , כלומר $ab\equiv 1(p)$ לכן ל b יש רק שתי אפשרויות $1,p-1$
  - p אי־זוגי ולכן $p-1$ זוגי $\Leftarrow$ ניתן לסדר את המספרים בסדרה $2,3...p-2$ בזוגות של הפכיים
  - על כן (הערה: הראנו שאין הכרח שהזוגות עוקבים/בהצלבות/חוקיות כלשהי):

$$2\cdot 3\cdot....\cdot(p-3)(p-2)\equiv 1(\mod p)$$

  - נכפיל ב $p-1$ ו ב 1 :

$$(p-1)!=1\cdot 2\cdot 3\cdot ....\cdot(p-3)(p-2)(p-1)\equiv(p-1)\cdot 1\cdot 1\equiv -1(\mod p)$$

0.2.12 וילסון הפוך: אם $(n-1)!\equiv -1(n)$ אז n ראשוני

- נניח בשלילה ש $(n-1)!\equiv -1(n)$ ו n פריק ־ לכן ישנם a,b כך ש $n=ab$ $2\le a,b<n$.
- בה"כ a מקיים ש:
  - $a<n \Leftarrow a|(n-1)!$
  - מנתון $a|n$, וגם $n|(n-1)!+1$
  - לכן: $a|(n-1)!+1$
- לכן $2\le a|(n-1)!+1-(n-1)!=1$, וזו סתירה!

0.2.13 פרמה הקטן: יהי p ראשוני ויהי $a\in\mathbb{Z}^+$ כך ש $p\nmid a$ אז $a^{p-1}\equiv 1(\mod p)$

<u>הוכחה:</u>

- תהיה $T=\{,2,3,....(p-1)\}$ מהגדרה זוהי מערכת שאריות שלמה
- נגדיר $S=\{a,2a,3a,....(p-1)a\}$
- <u>למה 1־ "0 לא נולד" : איברי S מיוצגים על ידי המחלקות $1,2,...p-1$ מודלו p:</u>
  - אם נניח בשלילה שקיים $j\in[1,p-1]$ כך ש $ja\equiv 0(p) \iff p|ja$ זו סתירה ל $p\nmid a$, ולכן אין אף איבר כזה.
- <u>למה 2 ־ "לא איבדנו אף נציג" : כל זוג איברים אינו שקולו מודלו p</u>
  - נניח בשלילה שישנם $k_1\neq k_2\in[1,n-1]$ כך ש: $ja\equiv ka(p)$
  - נתון כי $gcd(a,p)=1$ לכן מחלוקה מודלארית יתקיים ש:

$j\cancel{a} \equiv k\cancel{a}(p) \iff j \equiv k(\frac{p}{\gcd(p,a)}) \equiv j \equiv k(p) \iff j = k$ סתירה

- כעת:

$$(a)\,(2a)\,(3a)\ldots.(p-1)\,a = a^{p-1}(p-1)! \overset{1}{\equiv} (p-1)! \overset{2}{\equiv} 1 \pmod p$$

1. מהלמות. 2. מוילסון

0.2.14 מסקנה מפרמה: p **ראשוני ו** $a \in \mathbb{Z}^+$ $a^p \equiv a \pmod p$

הוכחה:

- אם $p|a$ אז $p|a^p$ ולכן $a^p \equiv a \equiv 0 \pmod p$
- אם $p \nmid a$ אז a, p עומדים בתנאי משפט פרמה הקטן, ולכן $a^{p-1} \equiv 1 \pmod p$
  - נכפול ב a , נקבל: $a^p \equiv a \pmod p$

0.2.15 מסקנה מפרמה: p **ראשוני ו** $a \in \mathbb{Z}^+$ $a^p \equiv a \pmod p$ **כך ש** $p|a$ **אז** a^{p-2} **הופכי ל** a **מודולו** p

הוכחה:

$$a^{p-1} \equiv 1 \pmod p \iff a \cdot a^{p-2} \equiv 1 \pmod p$$

0.2.16 משפט השאריות הסיני: יהיו $n_1, n_2, \ldots n_r$ **מספרים שלמים חיוביים שזרים בזוגות אז למערכת** $\left\{\begin{array}{c} x \equiv a_1(n_1) \\ x \equiv a_2(n_2) \\ \vdots \\ \\ x = \equiv a_r(n_r) \end{array}\right\}$ **אז**

למערכת קיים פתרון יחיד $\prod_{i=1}^{r} n_i$

הוכחה

קיום:

- נגדיר $x = \sum_{i=1}^{r} a_i M_i y_i$ כך:
  - a_i ־ נתון
  - $M_i = \frac{\prod_{k=1}^{r} n_k}{n_i} = \frac{n_1 \cdot n_2 \cdot \ldots \cdot \cancel{n_i} \cdot \ldots n_r}{\cancel{n_i}}$
  - y_i ־ הופכי מודלארי ל M_i מודולו n_i . נשים לב שההופכי מודלארי אכן קיים שכן $gcd(M_i, n_i) = 1$ מהגדרת M_i ומנתון שה nים זרים בזוגות
- נראה שאכן x פותר את המערכת:

יהיה $k \in [r]$ ונראה ש $x = a_k(n_k)$:

$$x = \sum_{i=1}^{r} a_i M_i y_i = a_1 M_1 y_1 + a_2 M_2 y_2 + ... + a_k M_k y_k + ... + a_r M_r y_r \equiv a_k (n_k)$$
$$\Downarrow$$
$$0(n_k) + 0(n_k) + ... + a_k M_k y_k + ... + 0(n_k) \equiv a_k(n_k)$$
$$\Downarrow$$
$$x \equiv a_k M_k y_k \overset{\substack{inverse \\ modular}}{\equiv} a_k \cdot 1 \equiv a_k(n_k)$$
$$\Downarrow$$
$$x \equiv a_k(n_k)$$

יחיד:

- נניח בשלילה שישנם שני פתרונות x_1, x_2 כך ש: $x_1 \not\equiv x_2 \left(\prod_{i=1}^{r} n_i\right)$
- לכן לכל $k \in [r]$ מתקיים ש: $x_1 \equiv x_2 \equiv a_k(n_k) \iff x_1 - x_2 \equiv a_k(n_k) \iff n_k | x_1 - x_2$
- לכן: אם נסמן $M = n_1 \cdot n_2 ..... \cdot n_r$ יתקיים ש: $M | \underbrace{x_1 - x_2}_{=m}$
- למה (מהתרגול): אם $n_1, ...n_r$ זרים בזוגות + $n_i | m$: $\forall i \in [r]$ $\Leftarrow \prod_{i=1}^{r} n_i | m$
- מלמה 1 : $M | x_1 - x_2 \iff \prod_{i=1}^{r} n_i | x_1 - x_2 \iff x_1 \equiv x_2 \left(\prod_{i=1}^{r} n_i\right)$ וזו סתירה.

קיום בעזרת אוילר (לשם התרגול)

- נגדיר $x = \sum_{i=1}^{r} a_i M_i$ כך:
  - a_i - נתון
  - $M_i = \frac{\prod_{k=1}^{r} n_k}{n_i} = \frac{n_1 \cdot n_2 \cdot .... \cancel{n_i} \cdot ... n_r}{\cancel{n_i}}$
- נראה שאכן x פותר את המערכת:

יהיה $k \in [r]$ ונראה ש $x = a_k(n_k)$:

$$x = \sum_{i=1}^{r} a_i M_i^{\varphi(n_i)} = a_1 M_1^{\varphi(n_1)} + a_2 M_2^{\varphi(n_2)} + ... + a_k M_k^{\varphi(n_k)} + ... + a_r M_r^{\varphi(n_r)} \equiv a_k(n_k)$$
$$\Downarrow$$
$$0(n_k) + 0(n_k) + ... + a_k M_k^{\varphi(n_k)} + ... + 0(n_k) \equiv a_k(n_k)$$
$$\Downarrow$$
$$x \equiv a_k M_k^{\varphi(n_k)} \overset{\text{Euler}}{\equiv} a_k \cdot 1 \equiv a_k(n_k)$$
$$\Downarrow$$
$$x \equiv a_k(n_k)$$

הגדרות:

- נאמר שמספר n פריק הוא **פסודו־ראשוני** מבסיס b אם $b^n \equiv b(n)$
- נאמר שמספר פריק n הוא **מספר קרמייקל** אם $b^{n-1} \equiv 1(n)$ לכל $b \in \mathbb{Z}$ שזר ל n.
- יהיה $n \in \mathbb{Z}^+$ נאמר ש $\varphi(n)$ היא כמות המספרים הטבעיים הקטנים מ n שזרים אליו, כלומר $\varphi(n) = |\{k \in [n] : \ gcd(k, n) = 1\}|$
- נאמר ש f **פונקציה כפלית** אם $f(mn) = f(m)f(n)$ לכל m, n זרים.
  - נאמר ש f **פונקציה כפלית שלמה** אם מתקיים לכל $n, m \in \mathbb{Z}^+$

0.2.17 משפט: יהיה $\left\{\begin{array}{c} n=q_1.....q_k \\ \{q_i\}_i^k \ \textbf{primes} \\ \forall j\in[k] \ \ q_j-1|n-1 \end{array}\right\}$ **אז n הוא מספר קרמייקל**

<u>הוכחה:</u>

- יהי $b\in\mathbb{Z}$ זר ל n <u>צ"ל</u> ש $b^{n-1}\equiv 1(n)$
- מנתון ש b זר ל n נובע ש b זר גם לפירוק שלו כלומר $gcd(q_j,b)=1$ לכל $j\in[k]$
- מפרמה $b^{q_j-1}\equiv 1(q_j) \iff q_j|b^{q_j-1}-1$
- נתון שלכל $j\in[k]$ $q_j-1|n-1 \iff (q_j-1)\,t_j=n-1$ עבור $t_j\in\mathbb{Z}$
- אז:

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

- לכן:

$$b^{n-1}\equiv 1(q_1q_2....q_k)\equiv 1$$

0.2.18 יהיו $a,n\in\mathbb{Z}^+$ זרים אם $r_1,r_2,....r_{\varphi(n)}$ היא מערכת שאריות מצומצת מודולו n אז גם $a\cdot r_1,a\cdot r_2,......ar_{\varphi(n)}$ גם מערכת שאריות מצומצת מודלות n

<u>הוכחה:</u>

- <u>"0 לא נולד" - כל איבר זר ל n :</u>
  - יהי $j\in[\varphi(n)]$ ונניח בשלילה ש $ar_j\equiv 0(n) \iff n|ar_j$ אז $a|n$ סתירה לנתון
- <u>"לא איבדנו אף נציג" - כל שני מספרים אינם שקולים מודלו n :</u>
  - נניח בשלילה שישנם $k\neq j\in[\varphi(n)]$ כך ש $ar_j\equiv ar_k\,(n) \iff r_j\equiv r_k\,(n)$ כי $gcd(a,n)=1$
  - מכך ש $r_1,...r_{\varphi(n)}$ מערכת שאריות מצומצת נבוע $r_j\equiv r_k(n)$ אם"ם $j=k$, וזו סתירה

<u>מסקנה:</u>

$$(a\cdot r_1)(a\cdot r_2)......(ar_{\varphi(n)})\equiv r_1r_2,....r_{\varphi(n)}(n)$$

<u>הסבר:</u>

- יש אותה כמות איברים בשני צדי המשוואה
- לכל איבר יש איבר שקול בצד שני
- והאיברים בכל צד זרים בזוגות

0.2.19 משפט אוילר: עבור $a,n\in\mathbb{Z}^+$ זרים $\Leftarrow$ $a^{\varphi(n)}=1(n)$

<u>הוכחה:</u>

- מטענה קודמת עבור מערכת שאריות שלמה מתקיים:

$$(a\cdot r_1)(a\cdot r_2)......(ar_{\varphi(n)})\equiv r_1r_2,....r_{\varphi(n)}(n)$$

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

- כיון וזוהי מערכת שאריות שלמה, לכל r_i זר n , ולכן מחלוקה מודלארית:

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

0.2.20 מסקנה: $n \in \mathbb{Z}^+$ **ו** $a \in \mathbb{Z}$ **ו־** a, n **זרים** $\Leftarrow$ $a \cdot a^{\varphi(n)-1} \equiv 1(n)$ **(מחוקי חזקות)**

0.2.21 לכל n **ראשוני מתקיים** $\varphi(n) = n - 1$

<u>הוכחה:</u>

- מהגדרה:$\varphi(n) = |\{k \in [n] :\ gcd(k, n) = 1\}|$ ולכן יש לכל היותר n איברים
- מהגדרה $gcd(n, n) = n$ לכן $n \notin \varphi(n)$
- מהגדרה לכל $k \in [1, n-1]$ יתקיים ש: $gcd(k, n) = 1$, ויש $n - 1$ איברים באינטרוול.

0.2.22 לכל n **פריק** $\varphi(n) \leq n - 2$

<u>הוכחה:</u>

- נתון n פריק, ולכן קיים לפחות d אחד, $2 \leq d < n$ ולכן $d \notin \varphi(n)$
- מלמה קודמת גם n לא נספר
- לכן $\varphi(n) \leq n - 2$

0.2.23 יהי p **ראשוני ויהי** $k > 0$ **אז :** $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$

<u>הוכחה:</u>

- מהגדרת פונקציית אוילר ־ וחיסור קבוצות:

$$\varphi(p^k) = \left|\left\{k \in \left[p^k\right] :\ gcd(k, p^k) = 1\right\}\right| = \left|\left[p^k\right] \setminus \left\{k \in \left[p^k\right] :\ k|p^k\right\}\right|$$

- ממשפט החלוקה:

$$= \left|\left[p^k\right] \setminus \left\{\overset{m \in p^{k-1} \cap \mathbb{Z}}{k \in \left[p^k\right]} :\ km = p^k\right\}\right| = \left|\left[p^k\right] \setminus \left\{\overset{m \in p^{k-1} \cap \mathbb{Z}}{k \in \left[p^k\right]} :\ pm = p^k\right\}\right|$$

- $k = p$ כיון שרק כפולות של מספרים אלו יכולת להגיע לחזקות של p, לכן:

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

0.2.24 $\varphi(n) = \prod_{i=1}^{k} \varphi\left(p_i^{a_i}\right) = n \prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right)$

$\varphi(n)$ **פונקציה כפלית**

- יהיו m, n זרים אז:

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

1. מהמשפט $gcd(a,b)=1 \wedge gcd(a,c)=1 \iff gcd(a,bc)$

- לכן אם נספור את כמות האיברים שזרים ל m וגם ל n , סיימנו
- מכיון ויש לנו $m\times n$ איברים נוכל לסדרם במטריצה:

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

- נשים לב שבכל שורה מספר האיברים שזרים ל m הוא $\varphi(m)$ לכן נותרנו עם $n\cdot\varphi(m)$ איברים
- תהיה עמודה כלשהי: $\begin{matrix}\boldsymbol{r}\\ \boldsymbol{m+r}\\ \vdots\\ \boldsymbol{qm+r}\\ \vdots\\ \boldsymbol{(n-1)\,m+4}\end{matrix}$ (בעמודה יש n איברים)
- מלמה בעבור האלגוריתם של אקולידס מתקיים ש $gcd(qm+r,m)=gcd(r,m)$
- ולכן נשאל מהם האיברים $gcd(qm+r,m)=gcd(r,m)=1$, ולכן יש $\varphi(n)$ איברים בכל עמודה.
  - הוכחנת: יהי $r\in[m]$ כך ש $gcd(r,m)=1$ ונניח בשלילה שישנם $q_1\neq q_2\in[0,n-1] \Leftarrow q_1\not\equiv q_2(n)$
  - מכך ש n,m זרים: $q_1m+r\equiv q_2m+r(n) \iff q_1m\equiv q_2m(n) \iff q_1\equiv q_2(n)q_1$ וזו סתירה.
- ולכן **בכל** המטריצה יש $\varphi(n)\varphi(m)$ איברים איברים שזרים ל m ו ל n
- ולכן $\varphi(m\cdot n)=\varphi(n)\varphi(m)$, כנדרש

כעת יהי $n\in\mathbb{Z}^+$:

- מהמשפט היסודי לאריתמטיקה $n=\prod_{i=1}^{k}p_i^{a_i}$
- מכיון ו $\varphi(n)$ כפלית: $\varphi(n)=\prod_{i=1}^{k}\varphi\left(p_i^{a_i}\right)$
- ממשפט עבור פונקציית אוילר על מספר ראשוני: $\prod_{i=1}^{k}\varphi\left(p_i^{a_i}\right)=\prod_{i=1}^{k}p_i\left(1-\frac{1}{p_i}\right)=n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$
- בסה"כ: $\varphi(n)=\prod_{i=1}^{k}\varphi\left(p_i^{a_i}\right)=n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$

0.3 RSA

0.3.1 אלגוריתם:

1. בחר שני מספרים ראשוניים (ענקיים)
2. הגדר $n=qp$ וחשב $\varphi(n)=(p-1)\,(q-1)$

3. בחר מספר e אי זוגי, כך ש: $gcd\left(1,\varphi\left(n\right)\right)=1$ (כיצד? ילמד באלגוריתמים)
4. בחר d הופכי לe מודלו $\varphi(n)$ כלומר $de\equiv 1\left(\mod \varphi(n)\right)$
5. הגדר:
   - $\langle e,n\rangle$ - מפתח ציבורי
   - $\langle d,n\rangle$ - מפתח פרטי
6. הגדר את הפונקציות - m זה המסר:
   - $P_A(m)=m^e\equiv m\left(\mod n\right)$
   - $S_A(m):=m^d\equiv m\left(\mod n\right)$

0.3.2 טענה: $P_A\left(S_A(m)\right)=S_A\left(P_A(m)\right)$

מתקיים ש:

$$P_A\left(S_A(m)\right)\overset{6}{=}\left[P_A\left(m^d\right)\right]_n\overset{6}{=}\left[\left(m^d\right)^e\right]_n\overset{\text{power rules}}{=}\left[\left(m^e\right)^d\right]_n\overset{6}{=}\left[S_A\left(m^e\right)\right]_n\overset{6}{=}S_A\left(P_A(m)\right)$$

0.3.3 טענה: $P_A\left(S_A(m)\right)=m=S_A\left(P_A(m)\right)$

הראנו: $P_A\left(S_A(m)\right)=\left[m^{de}\right]_n=S_A\left(P_A(m)\right)$ אם נראה ש: $m^{de}\equiv m(n)$ סיימנו.
לכן:

- הראנו בכיתה שאם $c|ba$ ו b,a זרים אז $c|a$ וגם $c|a$ לכן מספיק להראות ש:

$$m^{de}\equiv m(n)\iff m^{de}\equiv m(qp)\iff m^{de}\equiv m(p)\wedge m^{de}\equiv m(q)$$

- נתבונן ב $m^{de}\equiv m(p)$:
  - מסעיף 4 באלגוריתם מתקיים ש: $de=1\left(\mod \varphi\left(n\right)\right)\iff de=k(p-1)(q-1)+1$
  - נציב:

$$m^{de}\equiv m^{k(p-1)(q-1)+1}\equiv m\cdot m^{(p-1)^{k(q-1)}}\left(\mod p\right)\overset{Fermat}{\equiv}m\cdot 1^{k(q-1)}\equiv m\cdot 1\equiv m\left(\mod p\right)$$

כנדרש

- נתבונן ב $m^{de}\equiv m(q)$
  - סימטרי

0.3.4 המסננת של ארסטותנס

```
Sieve(n):
    for k:2→ n
        A[k]=1;
    for k:2→ √n:
        if(A[k] == 1
            i=2k;
              while(i <= n):
                A[i] = 0
                i= i + k ;
```

טענה: בסיום $A[k]=1 \iff k$ **ראשוני**

0.3.5 אלגוריתם חזקה מודלארית

```
pow_mod(a,e,n)
    if e == 0
        return 1
    if e % 2 == 0 (is even?)
        t = pow_mod(a,e/2,n)
        return t^2 % n
    else
        t = pow_mod(a, e-1, n )
        return a*t % n
```

הוכחה:

על פי פעולת האלגוריתם: $a^e = \begin{cases} a\cdot a^{e-1} & \text{e odd} \\ \left(a^{\frac{e}{2}}\right)^2 & \text{e even}\end{cases}$, ומחוקי חזקות הביטוי תקין. נראה באינדוקציה:

<u>בסיס:</u> עבור $e=0$: אז $a^0=1$ ✓

<u>צעד:</u> נניח לכל $d<e$ ונוכיח ל e

- <u>אם e אי זוגי:</u>
  - אז ניתן לבטא את $e=2k+1$ ויתבצע $t=pow\_mod(a,e-1,n)$ שמהנחת האינדוקציה t מקבל ערך תקין
  - ולכן ונחזיר $a\cdot t=a\cdot a^{e-1}=[[a^e]_n$, כנדרש
- <u>אם eזוגי:</u>
  - אז ניתן לבטא את $e=2k$ ויתבצע $t=pow\_mod(a,\frac{e}{2},n)$ שמהנחת האינדוקציה t מקבל ערך תקין
  - ולכן נחזיר $t^2=\left(a^{\frac{e}{2}}\right)^2=[a^e]_n$, כנדרש.