אוניברסיטת אריאל בשומרון
אגף הבחינות

לפני התחלת הבחינה, מלא את כל הפרטים הבאים בכתב ברור וקרא בעיון את ההוראות*:
(יש לשים לב, מחברות הבחינה נסרקות למאגר נתונים. יש להקפיד שלא לקפל/לתלוש/לכתוב בצבעים)

קוד נבחן | 5 | 1 | **מס' זהות** (העתק מכרטיס הנבחן/סטודנט) | 3 | 0 | 4 | 9 | 6 | 7 | 6 | 9 | 8 | **מחברת** _____ **מתוך** _____

שנה"ל תש 18 **סמסטר** א **מועד** א **תאריך הבחינה** 2 / 2 / 2016

שם המחלקה מקצי המחשב ומתמטיקה | **מס' הקורס** 7016910-2 | **שם הקורס** אורח המסברים

***לידיעת המרצה** - הסטודנט לא מסר את מחברת הבחינה בזמן שנקבע לבחינה זו.
אחר ב _____ **דקות. שם המשגיח:** _____

ציון	המחברת נבדקה ביום	שם המרצה	חתימת המרצה
95	3/02/2016	אלעזר חורב	

הוראות לנבחן

1. עליך להבחן בחדר בו הנך רשום
2. בהגיעך לאולם הבחינה הנח ליד המשגיח על הבחינה את חפציך האישיים הכוללים: תיקים, ספרים, מחברות, מכשיר אלקטרוני אחר ורשימות שונות. עליך להתיישב במקום שייקבע לך על ידי המשגיח.
   ***סטודנט שימצא ברשותו או בהישג ידו מכשיר סלולרי, או כל ציוד אלקטרוני אחר, יורחק לסימסטר אחד לפחות.**
3. אסור להחזיק בהישג יד חומר הקשור לבחינה/לקורס אלא אם הותר הדבר בכתב על ידי המרצה ורק בהתאם למותר.
4. סטודנט המקבל לידיו שאלון ואין בכוונתו להבחן, חובה עליו למלא את פרטיו האישיים ע"ג המחברת. עזב הסטודנט את האולם אחרי חלוקת השאלונים או לא מסר את מחברתו עם תום הבחינה, דינו כדין "נכשל" בבחינה.
5. יש להשמע להוראות המשגיח, אסור לשוחח או לעזוב את המקום או את חדר הבחינה ללא קבלת רשות המשגיח. הפונה בשאלה או בבקשה ירים את ידו.
6. קריאת השאלון מותרת רק לאחר קבלת רשות מהמשגיח.
7. משך זמן הבחינה מצוין בראש השאלון. עם הודעת המשגיח כי תם הזמן, על הנבחן להפסיק את הכתיבה, למסור את המחברת עם השאלון למשגיח, לחתום ליד שמו ברשימת הנבחנים ולצאת מאולם הבחינה.
8. יש לכתוב את התשובות בעט **בצבע כחול, או בצבע שחור** בלבד. **חל איסור מוחלט לכתוב בעיפרון.**
9. את הטיוטה, יש למחוק בהעברת קו.
10. בתום הבחינה, יש להשאיר את השאלון בתוך המחברת ולמסור אותו למשגיח.
    חל איסור לצלם ו/או להוציא שאלוני בחינה מחדר הבחינה.
11. מחברות בחינה נוספות לפי בקשת הנבחנים - יש למסור יחד עם המחברת הראשונה.
    מחברת הבחינה, שקיבל הנבחן, יהיו בפיקוחו ובאחריותו במשך כל הבחינה. בעת יציאה מן החדר יופקדו המחברות והשאלון בידי המשגיח.
12. **חל איסור מוחלט לתלוש דפים ממחברת הבחינה.**

מס.נבחן:5547228
7016910-2
חדר: 01.2.01
ת.ז. 304967698

ועדת המשמעת מזהירה!
נבחן שימצאו ברשותו חומרי עזר אסורים או יתפס בהעתקה, ייענש בחומרה.

הערה ראשונה - שעה ____ | **הערה שניה** - שעה ____

פסילת בחינה - שעה _____ שם _____ חתימה _____

שים לב! אין לכתוב מעבר לשוליים משני צידי הדף

* כל האמור בלשון זכר או בלשון נקבה מתייחס לגברים ולנשים כאחד.

30 - 1

20 - 2

20 - 3

4

25 - 4

1) $7x \equiv 11 \pmod{51}$ $\qquad (51,61)=(61,71)=(51,71)=1$

$8x \equiv 21 \pmod{61}$

$9x \equiv 31 \pmod{71}$

$\boxed{\text{נכון}}$

הוא! 51,61,71 אשוניים זרים, נפעיל את משפט השאריות הסיני

$M = 51\cdot 61\cdot 71 = 220{,}881$:(38 משפט)

$M_i = \frac{M}{m_i}$: $M_1 = 4331$ $\qquad M_2 = 3621$ $\qquad M_3 = 3111$

נמצא מספרים y_i הופכי של M_i:

I. $4331\, y_1 \equiv 1 \pmod{51} \Rightarrow 47 y_1 \equiv 1 \pmod{51}$ $\quad [4284 \equiv 0 \pmod{51}]$

$47 y_1 \equiv 1785+1 \pmod{51} \equiv 1786 \pmod{51}$

$(47,51)=1 \Rightarrow y_1 \equiv 38 \pmod{51}$

II. $3621\, y_2 \equiv 1 \pmod{61} \Rightarrow 22 y_2 \equiv 1 \pmod{61}$ $\quad [3599 \equiv 0 \pmod{61}]$

$22 y_2 \equiv 62 \pmod{61}$ $\qquad (22,61)=1 \Rightarrow 11 y_2 \equiv 31 \pmod{61}$

$11 y_2 \equiv 244+31 \pmod{61} \equiv 275 \pmod{61}$

$(11,61)=1 \Rightarrow y_2 \equiv 25 \pmod{61}$

III. $3111\, y_3 \equiv 1 \pmod{71} \Rightarrow 58 y_3 \equiv 1 \pmod{71}$ $\quad [3053 \equiv 0 \pmod{71}]$

$58 y_3 \equiv 3479+1 \pmod{71} \equiv 3480 \pmod{71}$

$(58,71)=1 \Rightarrow y_3 \equiv 60 \pmod{71}$

לפי משפט השאריות הסיני, יש פתרון יחיד X:

$X = 7\cdot 4331\cdot 38 + 8\cdot 3621\cdot 25 + 9\cdot 3111\cdot 60 \pmod{220{,}881}$

$X = 3{,}556{,}786 \equiv 22090 \pmod{220881}$

95/100 – כל הכבוד

אבל צריך/כדי לרשום קשר

שאפשר מי אתה/ה

אלעד.

1) I. $7x \equiv 11 \pmod{51} \Rightarrow 7x \overset{**}{\equiv} 255+11 \pmod{51} \equiv 266 \pmod{51}$

$(7,51)=1 \Rightarrow \underline{x \equiv 38 \pmod{51}}$ ✓

II. $8x \equiv 21 \pmod{61} \Rightarrow 8x \overset{**}{\equiv} 427+21 \pmod{61} \equiv 448 \pmod{61}$

$(8,61)=1 \Rightarrow \underline{x \equiv 56 \pmod{61}}$ ✓

III. $9x \equiv 31 \pmod{71} \Rightarrow 9x \overset{**}{\equiv} 284+31 \pmod{71} \equiv 315 \pmod{71}$

$(9,71)=1 \Rightarrow \underline{x \equiv 35 \pmod{71}}$ ✓

$M = 51 \cdot 61 \cdot 71 = 220881$ נרשם <u>לפי משפט השאריות הסיני (משפט 38)</u>

✓ (מתקיים כי $(51,61)=(61,71)=(71,51)=1$)

$M_i = \frac{M}{m_i} \Rightarrow M_1 = 4331 \quad M_2 = 3621 \quad M_3 = 3111$ ✓

נמצא עתה את y_i ההופכיים של M_i

$4331 y_1 \equiv 1 \pmod{51} \Rightarrow 4284 y_1 + 47 y_1 \overset{**}{\equiv} 7785+1 \pmod{51}$

$47 y_1 \equiv 7786 \pmod{51} \quad (47,51)=1 \overset{*}{\Rightarrow} \underline{y_1 \equiv 38 \pmod{51}}$

$3621 y_2 \equiv 1 \pmod{61} \Rightarrow 3599 y_2 + 22 y_2 \overset{**}{\equiv} 549+1 \pmod{61}$

$22 y_2 \equiv 550 \pmod{61} \quad (22,61)=1 \overset{*}{\Rightarrow} \underline{y_2 \equiv 25 \pmod{61}}$

$3111 y_3 \equiv 1 \pmod{71} \Rightarrow 3053 y_3 + 58 y_3 \overset{**}{\equiv} 3479+1 \pmod{71}$

$58 y_3 \equiv 3480 \pmod{71} \quad (58,71)=1 \overset{*}{\Rightarrow} \underline{y_3 \equiv 60 \pmod{71}}$

נרשם <u>לפי משפט השאריות הסיני (38)</u>: $x = \sum_{i=1}^{k} a_i M_i y_i$

$x = 38 \cdot 4331 \cdot 38 + 56 \cdot 3621 \cdot 25 + 35 \cdot 3111 \cdot 60 \pmod{220881}$ ✓

$x \equiv 185984 + 17{,}670{,}480 \pmod{220881}$

$\boxed{x \equiv 185984 \pmod{220881}}$ ✓

* כלומר $(a,m)=1$ ניתן לצמצם לא

במצבים m לכן לא מתקיים

** - לפי אריתמטיקה מודולרית

30/30

2) $d \nmid (a,b)$ אם $d \mid b$ ואם $d \mid a$ אז $a,b \neq 0 \in \mathbb{Z}$

1) (הוכחה באמצעות המשפט היסודי של האריתמטיקה.)

לפי המשפט היסודי של האריתמטיקה (דב בקלף):

$$a = q_1^{a_1} \cdot q_2^{a_2} \cdot q_3^{a_3} \cdot q_4^{a_4} \cdots q_n^{a_n}$$

$$b = p_1^{b_1} \cdot p_2^{b_2} \cdot p_3^{b_3} \cdot p_4^{b_4} \cdots p_n^{b_n}$$

הוא! $d \mid a$ הוא ש d

$$d = q_1^{a_1'} \cdot q_2^{a_2'} \cdots q_n^{a_n'}$$

הוא! $d \mid b$ הוא ש

$$d = p_1^{b_1'} \cdot p_2^{b_2'} \cdots p_n^{b_n'}$$

לכן, לכל $i \in [n]$ עבורו $a_i \neq 0$ נקבל $q_i = p_i$ (וגם $b_i \neq 0$)

נכתוב מחדש את d עם r הראשונים השונים מ־0:

$$d = p_1^{c_1} \cdot p_2^{c_2} \cdot p_3^{c_3} \cdots p_r^{c_r}$$

כאשר $c_r = a_i \neq 0$ עבור $1 \le r \le n$

כעת נכתוב את הגדרת ה־ gcd $E = (a,b)$

~~$E \mid a$ $E \mid b$~~

לפי הגדרת gcd, E הוא המחלק המשותף הגדול ביותר שלהם

לכן הוא מכיל את כל הראשוניים המשותפים ובחזקה המשותפת

הגבוהה ביותר. כלומר: $E = p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$

עבור כל הראשוניים

2) 1) $d \mid (a,b)$ אם $d \mid a$ ואם $d \mid b$ אזי $a,b \neq 0 \in \mathbb{Z}$

עפ"י המשפט היסודי של הארתמטיקה (דב בקלף):

$$a = q_1^{a_1} \cdot q_2^{a_2} \cdot q_3^{a_3} \cdots q_n^{a_n} \quad , \quad b = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$$

לפי הגדרת gcd (נסמן באות E):

$$E = q_i^{\min(a_i,b_i)} \cdot p_j^{\min(a_j,b_j)} \quad \forall i \in [n] \quad \forall j \in [r]$$

כלומר, E מכיל את כל הראשוניים המשותפים עם הקבוצה בחזקה המשותפת

נראה שכל d: $d \mid a$:

$$d = q_1^{a_1'} \cdot q_2^{a_2'} \cdots q_n^{a_n'}$$

עבור כל $i \in [n]$ עבורו $a_i \neq 0$. $d \mid b$:

$$d = p_1^{b_1'} \cdot p_2^{b_2'} \cdots p_r^{b_r'}$$

עבור כל $i \in [r]$ עבורו $b_i \neq 0$. הוא! $d \mid a$ וגם $d \mid b$ אזי הראשוניים

המופיעים ב־d משותפים ל־a ו־b לכן הם בהכרח יופיעו ב־E!

② ב) לפי משפט ה gcd המורחב (בר בדק): $E=\gcd(a,b)$

אזי קיימים x,y כך ש $E=ax+by$

יתרון: $d|a$! $d|b$ גם $d|E$

$d|a \Rightarrow$ קיים r כך ש $a=rd$.

$d|b \Rightarrow$ קיים s כך ש $b=sd$

10/10

סה"כ gcd המורחב: $E=ax+by$

$E=rdx+sdy=d(rx+sy)$

לכן $d|d(rx+sy)$ ולכן $d|E$ ■

③ א) $(a,5)=1 \Rightarrow 5|(a^{12}-1)$

5 primes

הוכחה! $(a,5)=1$ נסדר את משפט פרמה הקטן (מספר 40)

$a^{5-1}\equiv 1 \pmod 5 \Rightarrow a^4\equiv 1 \pmod 5$

נעלה את שני הצדדים בחזקת 3 ונקבל

$(a^4)^3\equiv 1^3 \pmod 5 \Rightarrow a^{12}\equiv 1 \pmod 5 \Rightarrow 5|a^{12}-1$ ■

לפי הגדרת קונגרואנטיות (מספר 26 בדף)

ב) $(a,7)=1 \Rightarrow 7|(a^{12}-1)$

7 primes

הוכחה! $(a,7)=1$ נסדר את משפט פרמה הקטן (מספר 40):

$a^{7-1}=a^6\equiv 1 \pmod 7 \Rightarrow (a^6)^2\equiv 1^2 \pmod 7$

$\Rightarrow a^{12}\equiv 1 \pmod 7 \Rightarrow 7|a^{12}-1$ ■ (משפט 26 בדף)

8

ג) $(a,35)=1 \Rightarrow 35|(a^{12}-1)$

הוכחה! $(a,35)=1$ אזי $(a,5)=1$ ו $(a,7)=1$ לכן נשתמש

בתוצאות הסעיפים הקודמים (א+ב) ונרשום

I. $a^{12}\equiv 1 \pmod 5$ II. $a^{12}\equiv 1 \pmod 7$

הוכחה! $(5,7)=1$ ולכן $\operatorname{lcm}(5,7)=35$. לכן, לפי Lemma

מספר בדף, נוכל להסיק את ה-mod:

4

I·II. $\Rightarrow a^{12}\equiv 1 \pmod{35} \Rightarrow 35|a^{12}-1$

לפי הגדרת קונגרואנטיות (משפט 6 בדף)

(4) א) primes $p>2$ $\Rightarrow$ $(2,p)=(-2,p)=1$

לפי למה 59: $\left(\frac{-4}{p}\right)=\left(\frac{-2}{p}\right)\cdot\left(\frac{2}{p}\right)$

לפי למה 61: $\left(\frac{-2}{p}\right)=\begin{cases}1 & p\equiv 1,3 \pmod 8\\ -1 & p\equiv 5,7 \pmod 8\end{cases}$

$\left(\frac{2}{p}\right)=\begin{cases}1 & p\equiv 1,7 \pmod 8\\ -1 & p\equiv 3,5 \pmod 8\end{cases}$

8/8

במקרה ב $\left(\frac{-2}{p}\right)=1$ ולכן $\left(\frac{2}{p}\right)=1$ עקב $\left(\frac{-4}{p}\right)=1$

במקרה ג $\left(\frac{-2}{p}\right)=-1$ ולכן $\left(\frac{2}{p}\right)=-1$ עקב $\left(\frac{-4}{p}\right)=1$

במקרה ד $-\left(\frac{2}{p}\right)=\left(\frac{-2}{p}\right)$ עקב $\left(\frac{-4}{p}\right)=-1$

לסיכום: $\left(\frac{-4}{p}\right)=\begin{cases}1 & p\equiv 1,5 \pmod 8\\ -1 & p\equiv 3,7 \pmod 8\end{cases}$ (4)

~~[illegible]~~

ב) $a_1, a_2, \dots, a_k \in 8n+5$

צ"ל: $(a_1\cdot a_2\cdot a_3\cdot\ldots\cdot a_k)^2+4\in 8n+5$

הוכחה: צריך שיקרה שלהם כי $(a_1\cdot a_2\cdot a_3\cdot\ldots\cdot a_k)^2\in 8n+1$

~~[illegible]~~ נכפל איברים מהצורה $8+5$ ונראה מה יקרה:

7/7

$(8n+5)(8k+5)=64nk+40k+40n+25=8(8nk+5k+5n+3)+1$

נעלה בריבוע את המכפלה ונראה מה יקבל:

$[(8n+5)(8k+5)]^2=[(64n^2+80n+25)(64k^2+80k+25)]$

$=4096n^2k^2+5120n^2k+1600n^2+5120nk^2+6400nk+2000n$

$+1600k^2+2000k+625$

$=8[512n^2k^2+640n^2k+200n^2+640nk^2+800nk+250n+200k^2+250k+78]+1$

לכן מכפלת איברים מהצורה $8+5$ והעלאה בריבוע יוצרים

מספר מהצורה $8+1$. לכן, כשמוסיפים 4 נשארים בצורה $8+5$ (4)

דרך א':

ג) בשלילה נניח כי ישנו מספר סופי של ראשוניים מהצורה 8n+5.

נסמן $S=\{q_1,q_2,q_3,\dots,q_k\}$ קבוצת כל הראשוניים מהצורה 8n+5. כעת נבחן את המספר $N=(q_1\cdot q_2\cdot\ldots\cdot q_k)^2+4$

המספר N הוא מהצורה 8n+5 (הוכח בסעיף ב') ולכן יש ראשוני q מהצורה 8n+5 המחלק אותו (מכפלת 8n+5* אינה מהצורה הזו) ולכן $q\in S$. ולכן $q\mid (q_1\cdot q_2\cdot\ldots\cdot q_k)^2$ וגם $q\mid N$ ולכן $q\mid N-(q_1\cdot q_2\cdot\ldots\cdot q_k)^2=4$ אבל זה אי אפשר כי q אי זוגי שאינו מהצורה 8n+5 סתירה. ∎

אולי כל הפקטורים מהצורה 8n+1, 8n+3 או 8n+7 אבל (8n+5)(8n+7)

דרך ב': נניח בשלילה כי ישנו מספר סופי של ראשוניים מהצורה 8n+5. נסמן $S=\{q_1,q_2,\dots,q_k\}$ קבוצת כל הראשוניים מהצורה הזו. נעבור לסתכל על המספר $N=(q_1\cdot q_2\cdot q_3\cdot\ldots\cdot q_k)$. N מהצורה 8n+5 (לפי סעיף ב'). כעת נסתכל על $N^2+4=(q_1\cdot\ldots\cdot q_k)^2+4$ מהצורה 8n+5 (לפי סעיף ב').

כעת נבחנו את הקונגרואנציה הבאה:

$N^2+4\equiv 0 \pmod q$

$N^2\equiv -4 \pmod q$

יש כאן לN שורש ריבועי modq אז $-1\equiv 5 \pmod 8$ (סעיף ג') בומר קיים 8n+5=q המחלק את N^2+4. לכן $q\in S$. לכן $N\mid q$ וגם $N^2\mid q$. אבל ידוע כי $N^2+4\mid q$ ולכן $4=N^2+4-N^2\mid q$. q ראשוני וגם 4|q לכן q=2 אבל $q\in 8n+5$ סתירה. ∎

* נבדוק מכפלת (8k+1)(8n+1)

$8n+1\in 64nk+8k+8n+1=8(8nk+k+n)+1$

לכן חייבת להיות לפחות q אחד מהצורה 8n+5 ודווקא אותו תפסנו בשבול הוכחה.

שים לב למה הוא קיים אולי הכל מהצורה 8n+1

15/10 על הניסוח. כיון היית צריך להגיב יאן

② א) סה"כ המספרים הראשוניים (מסדר 3 ב בדל):

$$a = q_1^{a_1} \cdot q_2^{a_2} \cdot q_3^{a_3} \cdot \ldots \cdot q_n^{a_n}$$

$$b = p_1^{b_1} \cdot p_2^{b_2} \cdot p_3^{b_3} \cdot \ldots \cdot p_r^{b_r}$$

כל מחלק משותף (e) יכול להשתמש רק ב a ו b בחזקה משותפת (קטנה יותר מ $\max(a_i, b_i)$).

לכן הגדר $d = \gcd(a,b)$ (למה 25) $d = q_1^{\min(a_i,b_i)} \cdot p_j^{\min(a_j,b_j)}$

מזמן d מכיל רק את המספרים הראשוניים המשותפים ל a,b ובחזקה המשותפת הגבוהה ביותר. לכן גם e|a וגם e|b

לכן בהגדרת $e \mid d = \gcd(a,b)$ ∎

10/10

~~מבחינת הלוגיקה טעות:~~

~~$e|a \Leftarrow a = er$; $e|b \Rightarrow b = et$~~

~~$d = (a,b) \Rightarrow \max(\text{כל המחלקים של } a \text{ ו } b) \Rightarrow d = \max(t,r,s,l\ldots)$~~

~~$N = (a_1 \cdot a_2 \cdot \ldots \cdot a_k) \Rightarrow N^2 = (a_1 \cdot a_2 \cdot \ldots \cdot a_k)^2$~~

~~$N^2 + 4 = (a_1 \cdot a_2 \cdot \ldots \cdot a_k)^2 + 4 \in 8n+5$~~

~~$N^2 + 4 \equiv 0 \pmod{8n+5}$~~ $\quad N^2 \equiv -4 \pmod{q}$

~~$\left(\frac{-4}{q}\right) = 1 \Rightarrow q = 1 + 8k$~~

~~או~~

~~$q = 5 + 8k$~~

יפה מאוד, גיין 95 סופית

משהו הכי לשם!

דור עימי קשר כדי שאדע

מי אתה המשך קבלת

הלימודים אלעד.

אליניר דיגיטל
עוצמת הדפוס הדיגיטלי
03-6240810