בס"ד

בחינה לדוגמה בתורת המספרים האלגוריתמית

סמסטר ב' תש"פ

חומר עזר מותר לשימוש: מחשבון מדעי פשוט

זמן: 3 שעות

הנחיות לגבי אופן כתיבת הבחינה:

א. בשאלות הפתוחות מותר להסתמך על משפטים שהוכחנו בהרצאה/תירגול, אם מצטטים אותם במדוייק (או כותבים את שמם כגון "משפט וילסון"), ובלבד שהמשפט המדובר הוא לא עיקר מה שצריך להוכיח באותה שאלה.

ב. את התשובות לשאלות האמריקאיות יש לרשום בעמוד הראשון של מחברת הבחינה ברצף. כגון:

1- א

2- ב

3- ג...

ואת החישובים והדרך יש לפרט בעמודים הבאים אך לסמן מעליהם קו אלכסוני ולרשום בראש הדפים "טיוטה".

החישובים הללו לא ישפיעו על הניקוד, אך נתבקשתי מטעם המחלקה לדרוש את קיומם לצורך איתור העתקות. לגיטימי שסטודנט יכתוב בתור פירוט הדרך "לא ידעתי וניחשתי", אך אם סטודנט ינמק 8 שאלות בניחוש ויצדק בכולן, הוא כנראה מתאים יותר להמשיך את לימודיו באוניברסיטת הוגוורטס.

הערות חשובות:

1. בעקבות המצב החריג הסמסטר, עדיין אין ודאות סופית לגבי אופן קיום הבחינה. לפיכך ייתכנו שינויים כמו שינוי כמות הזמן ובעקבותיו כמות או אורך השאלות, חלוקת הניקוד וכדומה. אם יהיה שינוי משמעותי מסוג זה, אעדכן בע"ה ברגע שאדע עליו.
2. בכמה מן השאלות האמריקאיות החישוביות, השתדלתי בבחינה לדוגמה לקחת שאלות עם אותם מספרים שעשינו בהרצאה, כדי שתוכלו להשוות את דרך הפתרון עם סיכומי ההרצאות. כמובן שאם שאלה כזו תופיע בבחינה היא תופיע עם מספרים אחרים.
3. החלוקה לתת סעיפים בתוך שאלה (רלוונטי בעיקר לשאלות הפתוחות) וחלוקת הניקוד בין סעיפים, יכולות להשתנות בהתאם לאופי השאלה.

בהצלחה!

חלק א' – שאלות אמריקאיות – 10 נקודות לכל שאלה

1. יהי $d_1 = \gcd(341,319)$ ו- $d_2 = \gcd(187,253)$. למה שווה הסכום $d_1 + d_2$?

א. 31

ב. 22

ג. 11

ד. 12

בס"ד

2. מצאו $x, y \in Z$ כך ש- $9x - 15y = 12$. חובה למצוא אותם באמצעות השיטה שלמדנו בהרצאה המשתמשת באלגוריתם אוקלידס המוכלל. (אחרת ייתכנו תשובות רבות...) למה שווה הסכום $x + y$?

א. 10

ב. 11

ג. 12

ד. 67

3. ההוכחה של אוקלידס לקיומם של אינסוף ראשוניים:

א. מתבססת על המשפט הקטן של פרמה.

ב. מבוססת על כך שאם נוסיף למכפלת n הראשוניים הראשונים 1, נגלה שקיים ראשוני נוסף.

ג. מהווה הוכחה נוספת למשפט החלוקה.

ד. מבוססת על חלוקת הראשוניים (הגדולים מ-2) לשתי מחלקות לפי השארית שלהם מודולו 4.

4. נתונים שני היגדים:

היגד ראשון: יהיו $a, b \in Z$ לא שניהם 0. $d = \gcd(a, b)$ אם"ם לכל c שלם כך ש- $c|a$ וגם $c|b$ מתקיים $c|d$.

היגד שני: 341 פסאודו ראשוני לפי בסיס 2.

א. ההיגד הראשון אמת והשני שקר
ב. ההיגד הראשון אמת והשני אמת.
ג. ההיגד הראשון שקר והשני שקר
ד. ההיגד הראשון שקר והשני אמת.

5. נתונים שני היגדים עבור $a, b \in Z$ ו- $k, m \in N$:

היגד ראשון: $a \equiv b(mod\ m) \Leftarrow a^k \equiv b^k(mod\ m)$

היגד שני: $a \equiv b(mod\ m) \Rightarrow a^k \equiv b^k(mod\ m)$

א. ההיגד הראשון אמת והשני שקר
ב. ההיגד הראשון אמת והשני אמת.
ג. ההיגד הראשון שקר והשני שקר
ד. ההיגד הראשון שקר והשני אמת.

6. מצאו פתרון $0 \le x < 105$ למערכת השקילויות הבאה:

$$x \equiv 1(mod\ 3)$$

$$x \equiv 2(mod\ 5)$$

$$x \equiv 3(mod\ 7)$$

למה שקול x שקיבלתם מודולו 4?

א. 0
ב. 1
ג. 2
ד. 3

7. נתון בקיצור אלגוריתם ה-RSA:

- p, q ראשוניים, $n = pq$.
- מצא e כך ש-$(e, \varphi(n)) = 1$.
- מצא d כך ש-$de \equiv 1(mod\ \varphi(n))$.
- מפתח ציבורי: $P_a(m) = m^e(mod\ n)$ מפתח פרטי: $S_a(m) = m^d(mod\ n)$.

מה אפשר לומר על הפונקציות $P_a(m), S_a(m)$?

א. הפכיות זו לזו (מודולו n).
ב. לכל m זר ל-n מתקיים $P_a(m) \equiv S_a(m)\ \ (mod\ \ \varphi(n))$.
ג. אינן תלויות בבחירה של e.
ד. כל התשובות נכונות.

8. . נתונים שני היגדים:

היגד ראשון: תהי G חבורה עם נייטרלי e ו-$g \in G$. אז קיים n טבעי כך ש-$g^n = e$.

היגד שני: אם p ראשוני, $a, b, c \in Z$ ומתקיים $ac \equiv bc(mod\ p)$ אזי $a \equiv b(mod\ p)$.

א. ההיגד הראשון אמת והשני שקר
ב. ההיגד הראשון אמת והשני אמת.
ג. ההיגד הראשון שקר והשני שקר
ד. ההיגד הראשון שקר והשני אמת.

<u>חלק ב – שאלה פתוחה, 15 נקודות</u>

9. א. נסחו והוכיחו את משפט וילסון ואת המשפט ההפוך למשפט וילסון.

ב. יהי p ראשוני, ונניח שגם $p + 2$ ראשוני. הוכיחו כי

$$4\big((p-1)! + 1\big) + p \equiv 0\ \big(\mathrm{mod}\ p(p+2)\big)$$

בס"ד

<u>חלק ג – שאלת הבנה – 5 נקודות</u> (השאלה המופיעה כאן לקוחה מבחינת סמסטר א' מועד א' השנה)

בשאלה זו הינכם מתבקשים להוכיח את הטענה הבאה.

<u>טענה:</u>

יהי $2 \le a \in \mathbb{N}$ ויהי p ראשוני אי-זוגי כך ש $p \nmid a^2-1$. אזי המספר $n := \dfrac{a^{2p}-1}{a^2-1}$ הינו פסודו-ראשוני לפי בסיס a.

הסעיפים הבאים מנחים אתכם בהוכחת טענה זו
שאלה זו.

סעיף א: הוכיחו כי n המוגדר לעיל הינו שלם ופריק.

בסעיף זה הינכם יכולים להסתמך על העובדה ש $x+1 \mid x^k+1$ לכל $k \in \mathbb{N}$ אי-זוגי וכל $x \in \mathbb{N}$.
אין צורך להוכיח עובדה זו.

סעיף ב: יהי p ראשוני אי-זוגי כך ש $p \nmid a^2-1$. הוכיחו כי $p \mid n-1$ וגם $2 \mid n-1$.

סעיף ג: יהי p ראשוני אי-זוגי כך ש $p \nmid a^2-1$. הוכיחו כי $a^{2p}-1 \mid a^{n-1}-1$.

סעיף ד: הוכיחו את הטענה המופיעה בראש שאלה זו.

<u>פתרונות</u>

1-ב

2-ג

3 -ב

4-ד

5 –א

6-א

7-א

8-ג

9 – סעיף א' בסיכומי ההרצאות וסעיף ב' במטלה 4. (שימו לב כי במטלה הופיע רמז לשאלה, אך בבחינה הוא לא חייב להופיע, אחרי שכבר ראיתם אותו במטלה.)

10. בעמוד הבא

(א)

$$n=\frac{a^{2p}-1}{a^2-1}=\frac{(a^p-1)(a^p+1)}{(a-1)(a+1)}=\underbrace{\frac{a^p-1}{a-1}}_{a^{p-1}+a^{p-2}+\dots+1 \text{ שלם}>1}\cdot\underbrace{\frac{a^p+1}{a+1}}_{\text{שלם}>1 \text{ זה ברור}}$$

(ב) נראה $p\mid n-1$:

$$n-1=\frac{a^{2p}-1}{a^2-1}-1=\frac{a^{2p}-1-a^2+1}{a^2-1}=\frac{a^{2p}-a^2}{a^2-1}$$

לפי פרמה $a^p\equiv a\ (p)$ ⇐ $a^{2p}\equiv a^2\ (p)$ המונה מתחלק ב p (כי p ראשוני גדול)

ולכן $n-1$ מתחלק ב p.

נראה $2\mid n-1$:

$$n-1=\frac{a^{2p}-1}{a^2-1}-1=\frac{(a^2)^p-1}{a^2-1}-1=\frac{\cancel{(a^2-1)}\left((a^2)^{p-1}+(a^2)^{p-2}+\dots+\cancel{1}\right)}{\cancel{a^2-1}}-\cancel{1}$$

כמות הפרמים היא p, אי זוגי

אם a אי"ז אז פלוס מספר זוגי של אי זוגיים ונקבל זוגי.

אם a זוגי אז כל הפרמים זוגיים ונקבל זוגי.

(ג) נסמן ב r את כי $2\mid n-1$ כי $p\mid n-1$ ומכיוון ש $(p,2)=1$ נקבל כי $2p\mid n-1$

כלומר יש k שלם $\ni$ $n-1=2pk$ ⇐

$$a^{n-1}-1=(a^{2p})^k-1=(a^{2p}-1)\underbrace{\left((a^{2p})^{k-1}+(a^{2p})^{k-2}+\dots+1\right)}_{\text{שלם}>1}$$

ולכן $a^{2p}-1\mid a^{n-1}-1$

(ד) לפי סעיף א n פרים.

לפי סעיף ג $a^{2p}-1\mid a^{n-1}-1$

כמו כן $n\mid a^{2p}-1$ לפי הגדרת n כי $n=\frac{a^{2p}-1}{a^2-1}$

לכן $n\mid a^{n-1}-1$ ⇐ $a^{n-1}-1\equiv 0\ (n)$ ⇐ $a^{n-1}\equiv 1\ (n)$ ⇐ $a^n\equiv a\ (n)$

⇐ n פסאודו ראשוני לפי בסיס a.