הרצאה 2 - חשבון שאריות ואלגוריתם אוקלידס

26 באפריל 2019

1 תרגיל 1

1.1 סעיף א

מצאו את $(56,101)$ וכן $x,y\in\mathbb{Z}$ כך ש- $(56,101)=56x+101y$.
ניעזר באלגוריתם אוקלידס:

$$\begin{aligned}101&=56\times1+45\\56&=45\times1+11\\45&=11\times4+1\\11&=11\times1\end{aligned}$$

לכן מתקיים כי $(56,101)=1$
ניעזר בחישובים שביצענו על מנת למצוא תא x,y, נבצע ''הצבות לאחור'' עד שנגיע לכפולות של $101,56$'.

$$\begin{aligned}1&=45-4\times11=\\&=45-4\times(56-45)\\&=5\times45-4\times56\\&=5\times(101-56)-4\times56\\&=5\times101-9\times56\end{aligned}$$

ולכן מצאנו את $x=-9,y=5$.

1.2 סעיף ב

פתרו את המשוואה $56x=1$ ב-$\mathbb{Z}_{101}$. באופן שקול אפשר לכתוב $56x\equiv1(mod101)$
מסעיף א', למדנו כי מתקיים $-9\times56\equiv 5\times101-9\times56=1$ שכן ב- $\mathbb{Z}_{101}$ כפולות של 101 ''ייעלמו'' כי הן שוות 0.
סך הכל הפתרון הוא: $-9\equiv_{101}-9+101=92$.

1.3 סעיף ג

פתרו: $56x \equiv_{101} 10$.

יודעים כי $56 \times (-9) \equiv_{101} 1$ מהסעיפים הקודמים, ולכן אם נכפיל ב10 נקבל: $10 \equiv_{101} 56 \times 11 \times 56 \equiv_{101} (-90)$. ולכן $x = 11$.

2 שאלה 2

נתונה המשוואה $3x + 6 = 4$. פתרו אותה ב-

2.1 סעיף א - ב$\mathbb{Z}_7$.

נעביר אגפים על מנת לבודד את $3x$:

$3x = 4 - 6 = -2 \equiv_7 5$

נשים לב כי ההפכי של 3 ב-$\mathbb{Z}_7$ הוא 5, שגן מתקיים $3 \times 5 = 15 \equiv_7 1$ ולכן:

$$
\begin{aligned}
3 \times (3^{-1} \times 5) &= 5 \\
&= 3 \times (5 \times 5)
\end{aligned}
$$

ולכן מתקיים $5 \times 5 = 25 \equiv_7 4$ ולכן $x = 4$.

2.2 סעיף ב - ב$\mathbb{Z}_3$

כאן המשוואה היא $0 = 1$.

3 שאלה 3

3.1 סעיף א

מצאו את ספרת האחדות של 333^{333}. למעשה נרצה לחשב את $333^{333} mod(10)$.

אני יודעים כי כפל בmod(n) פועל באופן הבא: $x \cdot y(modn) = ((xmod(n)) \cdot (ymod(n)))mod(n)$

במקרה שלנו למעשה הביטוי שקול ל-$3^{333} mod(10)$.

אם נסתכל על החזקות של 3:

$3^0 = 1, 3^1 = 1, 3^2 = 9, 3^3 = 27 = 7, 3^4 = 81 = 1$

יש בחזקות מחזוריות, לכן נפשט בעזרת תכונה זו את החישוב:

$3^{333} = 3^{83 \times 4 + 1} = (3^4)^{83} \cdot 3 \equiv_{10} 3$

3.2 סעיף ב

מצאו את ספרת האחדות של 12^{84}.

זה שקול לחישוב: $2^{84} mod(10)$.

נבין איך נראות חזקות של 2:

$2^0 = 1, 2^2 = 4, 2^3 = 8, 2^4 = 16 = 6, 2^5 = 32 = 2$

מסקנה: כפל בחזקות של 2^4 לא משנה את ספרת האחדות.

$2^{84} = 2^{4\cdot 21} = (2^4)^{21} = 6$

ולכן ספרת האחדות היא 6.

3.3 סעיף ג

חשבו את: $25^{25} mod(18)$. זה שקול ל-$7^{25} mod(18)$.

נבין כיצד עובדות חזקות של 7 במודולו 18:

$7^1 \equiv_{18} 7, 7^2 \equiv_{18} 13, 7^3 = 343 = 1 + 19 \times 18 \equiv_{18} 1$

לכן נוכל לרשום

$7^{25} = (7^3)^8 \cdot 7 \equiv_{18} 1 \cdot 7 = 7$

4 שאלה 4

נוכיח כי $x \in \mathbb{N}$ שנכתב בצורה: $\sum_{i=0}^{n} 10^i x_i$ מתחלק ב-9 אם ורק אם סכום ספרותיו מחלק ב-9. נשים לב שהסכום המסובך זאת שיטה להפריד ספרות של מספר רגיל (x_i היא הספרה ה-i).

אם x מתחלק ב- 9 מתקיים

$$\begin{aligned} & x \equiv_9 0 \\ \text{from equivalnce} \iff & \sum_{i=0}^{n} 10^i x_i \equiv_9 0 \\ \text{modulo multiplication} \iff & \sum_{i=0}^{n} (10^i mod(9))(x^i mod(9)) \equiv_9 0 \\ \text{since } 10 \equiv_9 1 \iff & \sum_{i=0}^{n} 1 \cdot x_i \equiv_9 0 \end{aligned}$$

■

5 שאלה 5

הוכיחו כי אין פתרון בשלמים למשוואה:

$x^2 + y^2 = 2019$

נניח בשלילה כי קיים פתרון ונשים לבל עבודה כי אם יש פתרון, אז קיים גם פתרון בכל שארית, ובפרט במודלו 4. כלומר:

$x^2 + y^2 \equiv_4 3$.

כעת צמצמנו מאוד את קבוצת המספרים השלמים שעלינו לבדוק. נוכל לבדוק ידנית:

$x, y \in 0, 1, 2, 3$ ולכן: $x^2, y^2 \in \{0, 1, 4 \equiv_4 0, 3^2 \equiv_4 1\}$. הריבועים היחידים הם 0 ו-1. לכן לא נוכל לחבר 2 ריבועים ולקבל 3.

קיבלנו סתירה להנחה ולכן אין פתרון למשוואה.

6 שאלה 6