<u>תרגיל 1:</u>

הוכיחו כי $2^{20} \equiv 1 \ (mod\ 41\ )$

<u>פתרון:</u> נציג 2 דרכים לפתרון

<u>דרך א'</u>

<u>שלב ראשון:</u> נציג את הביטוי ע"י שקליות כלומר צ"ל כי $2^{20} \equiv 1 \ (mod\ 41\ )$

<u>שלב שני:</u> העלה בחזקות שקרובות למודלו

$$2^{20} \equiv (2^5)^4 \equiv (32)^4 \equiv (-9)^4 \equiv ((-9)^2)^2$$
$$\equiv (81)^2 \equiv (-1)^2$$
$$\equiv 1\ (\ mod\ 41)$$

<u>דרך ב'</u>

<u>שלב ראשון:</u> נציג את הביטוי ע"י שקליות כלומר צ"ל כי $2^{20} \equiv 1 \ (mod\ 41\ )$

<u>שלב שני:</u> נגיע ל 2^{20} ע"י העלאה של כפולות של הבסיס

<u>שלב שלישי:</u> ידוע כי $2^{20} = 2^{16} \cdot 2^4$ (פירוק של 20 לבינארי)

כעת נחשב את $2^{16}, 2^4$

$$2 \equiv 2\ (\ mod\ 41\ )$$
$$2^2 \equiv 2^2 \equiv 4\ (\ mod\ 41\ )$$
$$2^4 \equiv 4^2 \equiv 16\ (\ mod\ 41\ )$$
$$2^8 \equiv 16^2 \equiv 256 \equiv 10\ (\ mod\ 41\ )$$
$$2^{16} \equiv 10^2 \equiv 100 \equiv 18\ (mod\ 41\ )$$

<u>שלב רביעי:</u> נבצע מכפלה

$$2^{20} \equiv 2^{16} \cdot 2^4 \equiv 18 \cdot 16 \equiv 288 \equiv 1\ mod\ (\ 41\ )$$

<u>תרגיל 2:</u>

א. נתון ש- $n \equiv 3 \pmod 7$. מה ניתן להסיק על $n \bmod 14$? (8 נק')

ב. נתון ש- $t \equiv 3 \pmod{14}$. מה ניתן להסיק על $t \bmod 7$? (7 נק')

<u>פתרון:</u>

<u>סעיף א' :</u> ידוע כי $n \equiv 3\ (mod\ 7\ )$ ולכן $7 \mid n-3$ ולכן $n-3 = 7k : k \in \mathbb{Z}$ ולכן

$n = 7k+3$. כעת נחלק ל2 מקרים

<u>מקרה ראשון:</u> k זוגי ולכן $k = 2t : t \in \mathbb{Z}$

ולכן מתקיים כי $n = 14t+3$ ולכן $n \equiv 3\ (mod\ 14)$

<u>מקרה שני:</u> k אי זוגי ולכן $k = 2t+1 : t \in \mathbb{Z}$

ולכן מתקיים כי $n = 14t+10$ ולכן $n \equiv 10\ (mod\ 14)$ ולכן התשובה היא

$n \equiv 3\ (mod\ 14)$ או $n \equiv 10\ (mod\ 14)$

<u>סעיף ב' :</u> ידוע כי $t \equiv 3\ (\ mod\ 14\ )$ ולכן $14 \mid t-3$ ולכן $t-3 = 14k : k \in \mathbb{Z}$ ולכן

$$t \equiv 14k+3 \equiv 7(2k)+3 \equiv 3\ (mod\ 7)$$

<u>תרגיל 3:</u>

הוכיחו כי $27 \mid 2^{5n+1} + 5^{n+2}$

<u>פתרון:</u>

דרך מחשבה בתרגילים כאלה הוא קודם כל להעביר לשקליות, ולאחר מכן לנסות להגיע לאותו בסיס ע"י הוספה או החסרה של כפליות של המודלו.

צריך להוכיח כי $2^{5n+1} + 5^{n+2} \equiv 0\ (mod\ 27)$

- חשוב מאוד לשים לב כי זו אינה משוואה אלה שקילות, יש להגיע מאגף שמאל אל אגף ימין כלומר לצאת מ $2^{5n+1} + 5^{n+2}\ (mod\ 27)$ ולהגיע ל $0\ (mod\ 27)$

$$2^{5n+1} + 5^{n+2} \equiv 2 \cdot 2^{5n} + 25 \cdot 5^n \equiv 2 \cdot (32)^n + 25 \cdot 5^n \equiv$$

$$\equiv 2\cdot(32-27=5)^n+25\cdot 5^n\equiv 27\cdot 5^n\equiv 0\ (mod\ 27)$$

תרגיל 4:

מצאו את הספרה האחרונה של 333^{333}

פתרון:

קודם כל נשים לב כי $333^{333}=3^{333}\cdot 111^{333}$ ולכן

$$111\equiv 1\ (\,mod\ 10\,)\Rightarrow 111^{333}\equiv 1^{333}\equiv 1\ (\,mod\ 10)$$
$$3^{333}-3^{4\cdot 83+1}=(3^4)^{81}\cdot 3=81^{83}\cdot 3\equiv 1^{83}\cdot 3\ (\,mod\ 10\,)$$
$$333^{333}=3^{333}\cdot 111^{333}\equiv 3\ (\,mod\ 10\,)$$

לסיכום (בינתיים):

יהיו $a\equiv b\ (\,mod\ m\,)$ ו- $c\equiv d\ (\,mod\ m\,)$ ו- לכל $k\in\mathbb{Z}^+$ מתקיים:

0. היחס $\equiv$ הוא יחס שקילות
1. $m\mid a-b$ **2.** $a=b+k\cdot m$
3. $k\cdot m\equiv 0\ (\,mod\ m\,)$
4. $a\pm km\equiv b\ (\,mod\ m\,)$
5. $a\cdot c\equiv b\cdot d\ (\,mod\ m\,)$ **6.** $a\pm c\ \equiv b\pm d\ (\,mod\ m\,)$
7. $a^k\equiv b^k\ (\,mod\ m\,)$
אם $ac\equiv bc\ (\,mod\ m\,)$ **אזי** $a\equiv b\ (\,mod\,\frac{m}{(a,c)})$ <u>אבחנה:</u> **אם** $(c,m)=1$ **אזי** $a\equiv b\ (\,mod\ m\,)$ <u>אבחנה:</u> **אם** $ab\equiv 0\ (\,mod\ p\,)$ **כאשר** p **ראשוני אזי** $a\equiv 0\ (\,mod\ p\,)$ **או** $b\equiv 0\ (\,mod\ p\,)$

<u>יש לדעת להוכיח את כלל הטענות.</u>