

פתרון תרגיל 1

1. א) ע"פ אלגוריתם אוקלידס עם מקדמים:  $m=4, n=-1$  ואכן:  $\gcd(21,77) = 7 = 4 \cdot 21 - 77$ .

ב)  $3465 = 150 \cdot 23 + 15$ .

$150 = 10 \cdot 15 + 0$

לכן  $\gcd(3465,150) = 15$  ועפ"י האלגוריתם:

$m = 1, n = -23$  כלומר  $15 = 1 \cdot 3465 - 150 \cdot 23$

ג) מציאת  $\gcd(30,455)$  עפ"י האלגוריתם של אוקלידס:

$455 = 30 \cdot 15 + 5$

$30 = 6 \cdot 5 + 0$

לכן  $\gcd(455,30) = 5$

ועפ"י האלגוריתם נקבל ש:

כלומר  $m = -15, n = 1$ .  $5 = 455 \cdot 1 - 30 \cdot 15$

2. ניעזר בתכונה של  $\gcd$ :  $\gcd(am,an) = a \cdot \gcd(m,n)$

$(a/d, b/d) = 1$  אם  $d = \gcd(a,b)$  (לפי התכונה הנ"ל)  $d \cdot \gcd(a/d, b/d) = \gcd(a,b) = d$

3.

על פי החישובים למטה ואלגוריתם אוקלידס נקבל:

$(840,575) = (575,265) = (265,45) = (45,40) = 5$

$840 = 1 \cdot 575 + 265$

$575 = 2 \cdot 265 + 45$

$265 = 5 \cdot 45 + 40$

4.

נראה את הפתרון עבור  $c = p^e, b = p^w, a = p^q$  כש- $p$  ראשוני,  $q, w, e$  טבעיים. הפתרון הכללי (על ידי הצגת כל המספר כמכפלת חזקות של מספרים כלליים) נובע ממקרה זה (למה?).

$[b,c] = p^{\max(e,w)} \rightarrow (a,[b,c]) = p^{\min(q, \max(e,w))}$

$(a,b) = p^{\min(q,w)}, (a,c) = p^{\min(q,e)} \rightarrow [(a,b), (a,c)] = p^{\max(\min(q,w), \min(q,e))}$

ולכן נשאר להוכיח שלכל שלשת מספרים טבעיים  $q, w, e$  מתקיים:

$\min(q, \max(e,w)) = \max(\min(q,w), \min(q,e))$ . הוכיחו זאת (על ידי חלוקה למקרים לגבי  $(q, w, e)$ ).

5. קיימים מספרים שלמים:

$r, s$

$c = ar = bs$  כך ש:

$\gcd(a, b) = 1$  נתון ש:

$\Rightarrow \exists x, y$

$ax + by = 1$  כך ש:

$c = c \cdot 1 = c(ax + by) = acx + bcy = a(bs)x + b(ar)y = ab(sx + ry)$

$\Rightarrow ab/c$

6. א) מצאו  $x$  שלם חיובי כך ש-  $17x \equiv 1 \pmod{53}$ .  
 ב) מצאו  $a$  שלם כך ש-  $a \equiv 1 \pmod{11}$ ,  $a \equiv 2 \pmod{3}$ ,  $a \equiv 4 \pmod{5}$ .

6. א) ניתן לכתוב את המשוואה כ-  $17x + 53k = 1$ . מכיוון ש-  $(17, 53) = 1$ , נקבל, ע"פ אלגוריתם אוקלידס עם מקדמים, ש-  $x, k$  הם המקדמים של  $17, 53$  כאשר מציגים את 1 כצירוף לינארי שלהם. אזי  
 $53 = 3 \cdot 17 + 2 \rightarrow 2 = 53 - 3 \cdot 17$   
 $17 = 8 \cdot 2 + 1 \rightarrow 1 = 17 - 8 \cdot 2 = 17 - 8 \cdot (53 - 3 \cdot 17) = 25 \cdot 17 - 8 \cdot 53 \rightarrow x = 25$

ב) ראשית נפתור את מערכת המשוואות:  $x \equiv 1 \pmod{11}$ ,  $x \equiv 2 \pmod{3}$ .  
 מכיוון ש-  $(3, 11) = 1$  נקבל ש-  $2 \cdot 11 - 7 \cdot 3 = 1$ . לכן, פיתרון של שתי המשוואות הנ"ל הוא  
 $x = 2 \cdot 11 \cdot 2 + (-7 \cdot 3) \cdot 1 \pmod{33} = 44 - 21 \pmod{33} = 23 \pmod{33}$ .  
 לכן צריך לפתור עתה את מערכת המשוואות:  $a \equiv 23 \pmod{33}$ ,  $a \equiv 4 \pmod{5}$ .  
 מכיוון ש-  $(33, 5) = 1$  נקבל ש-  $2 \cdot 33 - 13 \cdot 5 = 1$ . לכן, פיתרון של שתי המשוואות הנ"ל הוא  
 $a = 2 \cdot 33 \cdot 4 + (-13 \cdot 5) \cdot 23 \pmod{33 \cdot 5} = 264 - 1495 \pmod{165} = -1231 \pmod{165}$

לכן  $a = -1231$  הוא פתרון של מערכת המשוואות הנ"ל (למשל -  
 $(-1231 \pmod{5}) = -1 \pmod{5} = 4 \pmod{5}$ ).

7. א) נציב  $n = k + 1$  ונבדוק עבור אילו  $k$  מתקיימת הטענה:

$$(k + 1)^2 - 7 = k^2 + 2k - 6$$

או נבדוק מתי  $k^2 + 2k - 6 = lk$  עבור  $l$  שלם:

$$k^2 + (2 - l)k - 6 = 0$$

$$k(k + 2 - l) = 6$$

ע"פ הפירוקים האפשריים של 6 למכפלת שלמים נקבל את האפשרויות הבאות:

$$k = \pm 1, k = \pm 2, k = \pm 3, k = \pm 6$$

ולכן  $n = \pm 2, 0, -1, 3, 4, -5$  או 7.

ב) נמצא  $s, t$  כך שלכל  $a$ -

(1)  $s(2a+1) + t(9a+4) = 1$ . למשל - ניקח -  $s=9, t=-2$ . אזי לכל  $a$  הצירוף הלינארי המינימלי של  $2a+1$  ושל  $9a+4$  הוא 1 ולכן ה- gcd הוא 1.