תרגול 1

הקדמה מתורת המספרים:
נדבר על $\mathbb{Z}$:
הגדרה: יהיו $m,n \in \mathbb{Z}$. נאמר שm מחלק את n, ונסמן $m|n$ אם קיים איזשהו $c \in \mathbb{Z}$, כך ש:

$$n = mc$$

לדוגמא: כל מספר מחלק את 0 כי: $c = 0$. $m \cdot 0 = 0$.
הערה: ייתכן ש$m|n$ אבל לא מתקיים ש$m < n$. למשל: $2|(-4)$.
אם m וn מספרים טבעיים, אז העובדה ש$m|n$ תגרור ש$m < n$.
תרגיל: הוכיחו שאם $m|n_1 \wedge m|n_2$ אז m מחלק כל צירוף שלהם: כלומר כל ביטוי מהצורה $an_1 + bn_2$. כאשר $a,b \in \mathbb{Z}$.
הוכחה: $m|n_1$ לכן קיים $c_1 \in \mathbb{Z}$ כך ש$mc_1 = n_1$.
$m|n_2$ לכן קיים $c_2 \in \mathbb{Z}$ כך ש$mc_2 = n_2$.
$an_1 + bn_2 = amc_1 + bmc_2 = m(ac_1 + bc_2)$ ובנוסף, $ac_1 + bc_2 \in \mathbb{Z}$.
לכן $m|(an_1 + bn_2)$.
משפט החילוק עם שארית:
לכל $m,n \in \mathbb{Z}$ קיימים $q,r \in \mathbb{Z}$ יחידים כך ש:

$$n = qm + r$$

ובנוסף, $0 \leq r < |m|$
הגדרה: מחלק משותף מקסימלי:

$$gcd(a,b) = \max\{m \in \mathbb{N} | m|a \wedge m|b\}$$

הערה: אם a,b שניהם 0 לא ניתן להגדיר.
סימון: (a,b)
דוגמא: $(18,12) = 6$
$(11,23) = 1$
$(11,0) = 11$
$(-12,8) = 4$
הערה: אם $(a,b) = 1$ נגיד שa וb "זרים".
משפט: לכל שני מספרים $a,b \in \mathbb{Z}$ מתקיים:

$$(a,b) = \min\{xa + yb | x,y \in \mathbb{Z}, xa + yb \in \mathbb{N}\}$$

לדוגמא: $(18,12) = 6 = 1 \cdot 18 + (-1) \cdot 12$
$(18,12) = 3 \cdot 18 + (-4) \cdot 12$

$$(11,23) = 1 \cdot 23 + (-2) \cdot 11$$

הערה: המקדמים של הצירוף לא בהכרח יחידים.
הוכחה: נסמן $d = (a,b)$.
ו $c = \min(\{xa + yb | x,y \in \mathbb{Z}\} \cap \mathbb{N})$
מהגדרת הgcd $d|a \wedge d|b$. לכן d מחלק כל צירוף לינארי שלהם. בפרט

$$d|c$$

$d \leq c$
מצד שני, אם נוכיח ש$c|a \wedge c|b$ אז מהגדרת gcd נקבל $c \leq d$.
נוכיח ש$c|a$:
ממשפט החילוק עם שארית, קיימים $q,r \in \mathbb{Z}$ כך ש$0 \leq r < |c|$

$$a = qc + r$$

מהגדרת c קיימים x,y כך ש: $c = xa + yb$

$$a = q(xa + yb) + r$$

$$r = a - q(xa + yb) = (1 - qx)a - qy \cdot b$$

כלומר r הוא צירוף של a,b והוא גדול שווה ל0 , וקטן ממש מc.
לכן r חייב להיות 0 מהגדרת c. (c הוא הצירוף החיובי המינימלי. אז לא יכול להיות שr חיובי).
$r = 0$ גורר ש$a = qc$ ולכן $c|a$.
באותו אופן בדיוק אפשר להראות ש$c|b$.
לכן $c \leq d$.
כלומר, $c = d$.
מש"ל.
מסקנות:
1. קיבלנו שלכל $a,b \in \mathbb{Z}$ (a,b) הוא צירוף שלהם.
2. $(a,b) = 1$ (כלומר, a וb זרים) אמ"ם 1 הוא צירוף שלהם.

תרגיל: אם $c|a \wedge c|b$ אז $c|(a,b)$.
הוכחה: (a,b) הוא צירוף של a וb וראינו התרגיל קודם שאם $c|a \wedge c|b$ אז c מחלק כל צירוף שלהם.
תרגיל: נניח ש$c|ab$, ו$(c,a) = 1$ אז $c|b$.
הוכחה: מכיוון ש$(c,a) = 1$ קיימים $x,y \in \mathbb{Z}$ כך ש:

$$xc + ya = 1$$

$c|ab$ זה אומר שקיים $q \in \mathbb{Z}$ כך ש$cq = ab$.

$$qxc + qya = q$$

$$xab + qya = q$$

אז $a|q$
ננסה משהו אחר: נכפיל את המשוואה בb:

$$bxc + bya = b$$

$$bxc + ycq = b$$

$$c(bx + yq) = b$$

לכן $c|b$.
מש"ל.
תרגיל: יהי q מספר ראשוני. (כלומר, המחלקים הטבעיים שלו הם רק 1 וq).
הוכיחו שאם $q|ab$ אז $q|a \vee q|b$.
הוכחה: אם $q|a$ סיימנו. אחרת q לא מחלק את a.
זה אומר שq זר לa. הסבר: (q, a) הוא מספר שמחלק גם את q וגם את a. בפרט, הוא מחלק את q. כלומר הוא שווה או ל1 או לq. אבל אם הוא שווה לq זה אומר ש$q|a$, בסתירה להנחה. לכן הוא שווה 1.
מהתרגיל הקודם, q זר לa, ובנוסף, $q|ab$, זה אומר ש$q|b$.
איך מוצאים gcd?
באמצעות אלגוריתם אוקלידס:
למה: נניח ש$m = qn + r$. אז $(m, n) = (n, r)$
הוכחה: נסמן $d = (m, n)$. $d|n$ מהגדרה. ו$d|r$ כי r צירוף לינארי של m, n.

$$r = 1 \cdot m - qn$$

לכן $d \leq (n, r) = c$.
$c|n$ מהגדרה, ו$c|m$ כי m צירוף לינארי של n וr.
ולכן $c \leq (n, m)$.
לכן $c = d$.
איך עובד אלגוריתם אוקלידס: נתונים m, n. בה"כ $n < m$. נעשה חילוק עם שארית של m בn ("מחלקים" את הגדול בקטן).

$$m = qn + r$$

ועכשיו אפשר לקחת את (n, r). שזה זוג מספרים יותר קטן.

ואפשר להמשיך בתהליך וכל פעם לקבל זוג של מספרים יותר קטנים.
נמשיך עד שנגיע לשארית 0.
דוגמא:

$$(53, 47) =?$$

$$53 = 1 \cdot 47 + 6$$

$$(47, 6) =?$$

$$47 = 7 \cdot 6 + 5$$

$$(6, 5) =?$$

$$6 = 1 \cdot 5 + 1$$

$$(5, 1) =?$$

$$5 = 5 \cdot 1 + 0$$

התשובה: 1. (כלומר, לוקחים את המשספר האחרון לפני שהגענו לשארית 0).
דוגמא נוספת:

$$(224, 63) =?$$

$$224 = 3 \cdot 63 + 35$$

$$(63, 35) =?$$

$$63 = 1 \cdot 35 + 28$$

$$(35, 28) =?$$

$$35 = 28 + 7$$

$$(28, 7)$$

$$28 = 4 \cdot 7 + 0$$

לכן $(224, 63) = 7$.

טענה: אמרנו קודם שהgcd של שני מספרים הוא הצירוף המינימלי שלהם. בפרט, הוא צירוף שלהם. באמצעות אלגוריתם אוקלידס, אפשר למצוא מקדמים שיתנו את הצירוף הנ"ל.

איך זה עובד?

בכל שלב נכתוב את השארית המתקבלת כצירוף של שני המספרים הקודמים.

נדגים עבור

$$(224, 63) = 7$$

$$224 = 3 \cdot 63 + 35$$

$$35 = 224 - 3 \cdot 63$$

$$63 = 1 \cdot 35 + 28$$

$$28 = 63 - 35$$

$$35 = 1 \cdot 28 + 7$$

$$7 = 35 - 28$$

$$28 = 63 - (224 - 3 \cdot 63) = -1 \cdot 224 + 4 \cdot 63$$

$$7 = 35 - 28 = (224 - 3 \cdot 63) - (-1 \cdot 224 + 4 \cdot 63) =$$

$$2 \cdot 224 - 7 \cdot 63$$

דוגמא נוספת:

$$(234, 61)$$

$$234 = 3 \cdot 61 + 51$$

$$61 = 1 \cdot 51 + 10$$

$$51 = 5 \cdot 10 + 1$$

כעת נבטא את 1 כצירוף של 234 ו61.

$$51 = 234 - 3 \cdot 61$$

$$10 = 61 - 51 = 61 - (234 - 3 \cdot 61) = 4 \cdot 61 - 234$$

$$1 = 51 - 5 \cdot 10 = (234 - 3 \cdot 61) - 5(4 \cdot 61 - 234) = 6 \cdot 234 - 23 \cdot 61$$

תזכורת: שקילות מודולו m:
יהי m מספר טבעי. נגיד ש $x \equiv y \mod m$ אם $m|x-y$.
כלומר, יש להם את אותה שארית חלוקה.
דוגמאות:

$$4 \equiv 7 \mod 3$$

$$4 \equiv 10 \mod 3$$

$$4 \equiv (-2) \mod 3$$

$$10 \equiv 5 \mod 5$$