תמר בר-און
$tamarnachshoni@gmail$
שעות קבלה- בתיאום מראש במייל.
אתרי הקורס- $math-wiki, moodle$.
ש"ב- למודל.
הקלטות תרגול וסיכום- $math-wiki$
חובות:
יש ש"ב- לא להגשה. אבל מאוד חשוב לעשות את שיעורי הבית.
יהיה בוחן באמצע סמסטר (אזור חנוכה).
לא בטוח שהבוחן יהיה מגן.
הקדמה על תורת המספרים:
$\mathbb{Z}$.
יחס החלוקה:
הגדרה: נגיד שx מחלק את y ונסמן $x|y$ אמ"ם קיים $k \in \mathbb{Z}$ כך ש:

$$xk = y$$

דוגמא: $2|6$ כי $k = 3$ ומתקיים: $2 \cdot 3 = 6$.
תרגיל: הוכיחו שאם $x|y, z$, אז הוא מחלק כל צירוף לינארי שלהם, כלומר כל ביטוי מהצורה

$$ay + bz, a, b \in \mathbb{Z}$$

הוכחה: $x|y$ כלומר קיים $k_1 \in \mathbb{Z}$ כך ש $xk_1 = y$. באותו אופן קיים k_2 כך ש$xk_2 = z$.

$$ay + bz = axk_1 + bxk_2 = x(ak_1 + bk_2)$$

לכן

$$x|(ay + bz)$$

משפט החילוק עם שארית:
יהיו $x, y \in \mathbb{Z}$. אז קיימים $q, r \in \mathbb{Z}$. יחידים כך ש:

$$x = qy + r$$

ו $0 \leq r < |y|$
הגדרה: מחלק משותף מקסימלי:
יהיו $x, y \in \mathbb{Z}$ שלא שניהם 0. המחלק המשותף המקסימלי שלהם מוגדר להיות:

$$gcd(x, y) = \max\{d : d|x \wedge d|y\}$$

הערה: לפעמים מבמנים רק (x, y).
דוגמאות:

$$(6, 4) = 2$$

$$(8,0) = 8$$

$$(7,13) = 1$$

הערה: שימו לב שמההגדרה נובע שgcd הוא תמיד חיובי.
טענה מגניבה:

$$gcd(x,y) = \min(\{ax+by : a,b \in \mathbb{Z}\} \cap \mathbb{N})$$

הוכחה: נסמן $d = gcd(x,y)$
$c = \min(\{ax+by\} \cap \mathbb{N})$
כיוון ראשון: $d \leq c$: הוכחנו שכמספר שמחלק גם את x וגם את y, מחלק כל צירוף שלהם.
$d|x \wedge d|y$ לכן $d|c$ כי הוא צירוף שלהם. ושניהם מספרים חיוביים מההגדרה לכן $d \leq c$.
כיוון שני: נוכיח ש$c|x \wedge c|y$.
נשתמש במשפט החילוק עם שארית:

$$x = qc + r$$

כאשר $0 \leq r < c$ ידוע שקיימים מספרים שלמים a, b כך ש:

$$c = ax + by$$

נציב במשוואת החילוק עם שארית:

$$x = q(ax+by) + r$$

$$r = x - qax - qby = (1-qa)x - qby$$

קיבלנו שr הוא צירוף של x וy, וידוע שהוא אי שלילי וקטן מc.
c מוגדר להיות הצירוף החיובי המינמלי. ולכן $r = 0$.
קיבלנו ש$x = qc$. כלומר $c|x$.
כנ"ל לגבי y. לכן $c|y$.
אז מהגדרת מחלק משותף מקסימלי, $c \leq d$.
לסיכום: $c = d$.
דוגמאות:
1. $(27,17) = 1$

$$29 \cdot 27 - 46 \cdot 17 = 1$$

זה אומר ש1 הוא צירוף של שניהם.
הערה: הgcd של שני מספרים הוא צירוף של שני המספרים, אבל המקדמים לא בהכרח יחידים.
דוגמא: $(6,4) = 2$

$$6 - 4 = 2$$

$$2 \cdot 4 + (-1) \cdot 6 = 2$$

מסקנה: אם איזשהו $c \in \mathbb{Z}$ מקיים: $c|x \wedge c|y$, אז $c|(x,y)$.
הוכחה: הוכחנו ש(x,y) הוא צירוף שלהם. ובתרגיל קודם היום הוכחנו שאם $c|x \wedge c|y$ אז הוא מחלק כל צירוף לינארי שלהם. לכן $c|(x,y)$
הגדרה: מספרים נקראים "זרים" אם הgcd שלהם הוא 1.
לדוגמא: $(27,17) = 1$ לכן 27 ו17 הם זרים.
מסקנה: x וy זרים אמ"ם 1 הוא צירוף לינארי שלהם.
הוכחה: $\Leftarrow$ אם x וy זרים אז $(x,y) = 1$. וראינו שgcd הוא צירוף של שני המספרים, לכן 1 הוא צירוף שלהם.
$\Rightarrow$: הוכחנו ש(x,y) הוא הצירוף הלינארי החיובי המינימלי שלהם. אז אם 1 הוא צירוף שלהם, הוא בהכרח הצירוף החיובי המינימלי שלהם.
תרגיל:
הוכיחו שאם $x|yz$ ובנוסף, $(x,y) = 1$ אז $x|z$.
הוכחה: מכיוון ש$x|yz$ זה אומר שיש איזשהו k שלם כך ש $xk = yz$.
נתון ש$(x,y) = 1$. לכן קיימים $a, b \in \mathbb{Z}$ כך ש

$$1 = ax + by$$

נכפיל את המשוואה בz. נקבל:

$$z = axz + byz$$

נציב $xk = yz$

$$z = axz + bxk = x(az + bk)$$

קיבלנו ש$x|z$.
תרגיל: יהי $p \in \mathbb{N}$ מספר ראשוני. (המחלקים החיוביים היחידים שלו הם 1 וp, והוא שונה מ1)
הוכיחו שאם $p|xy$ אז $p|x \vee p|y$.
הוכחה: אם $p|x$- סיימנו.
נניח ש$p \nmid x$.
$gcd(p,x)$ הוא מספר חיובי שמחלק את שניהם, בפרט מחלק את p, ולכן הוא שווה ל1 או לp.
אבל אמרנו שp לא מחלק את x. לכן $(p,x) = 1$.
נשתמש בתרגיל הקודם ונקבל ש$p|y$.
אלגוריתם אוקלידס למציאת מחלק משותף מקסימלי:
טענת עזר: אם

$$x = qy + r$$

אז

$$(x,y) = (y,r)$$

הוכחה: נסמן $c = (x, y), d = (y, r)$.
$d \leq c$: מהגדרה, $d|y, r$. x הוא צירוף לינארי של y וr, ולכן מתרגיל שעשינו היום, $d|x$.
אז קיבלנו ש$d|x \wedge d|y$, ולכן $d \leq c$, כי c הוא המקסימלי שמחלק את שניהם.
$c \leq d$: מהגדרה $c|x \wedge c|y$. נשים לב ש

$$r = x - qy$$

כלומר, r הוא צירוף לינארי של x וy.
לכן $c|r$.
אז $c|x \wedge c|r$, לכן $c \leq d$.
אלגוריתם אוקלידס הולך כך:
התונים שני מספרים x וy. נעשה חילוק עם שארית של הגדול בקטן (בערך מוחלט). נקבל

$$x = qy + r$$

$$(x, y) = (y, r)$$

קיבלנו זוג של שני מספרים יותר קטנים.
נמשיך עם התהליך.
עד שנקבל שארית 0.
המספר האחרון לפני שנקבל שארית 0 הוא הgcd.
דוגמא:

$$(53, 47) =?$$

$$53 = 47 + 6$$

$$(47, 6) =?$$

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

$$(6, 5) =?$$

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

$$(5, 1)$$

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

$$(1, 0) = 1$$

$$(224, 63) =?$$

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

$$(63, 35) =?$$

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

$$(35, 28) =?$$

$$35 = 28 + 7$$

$$(28, 7)$$

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

לכן $(224, 63) = 7$.
הערה: באמצעות האלגוריתם נוכל גם למצוא מקדמים שיבטאו את $gcd(x, y)$ כצירוף לינארי של x וy.
הסבר: בכל שלב, נבטא את השארית המתקבל כצירוף של שני המספרים הקודמים.
ואז נשתמש בהצבות חוזרות בשביל לקבל את הgcd כצירוף של שני המספרים ההתחלתיים.

$$(234, 61) =?$$

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

$$(61, 51) =?$$

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

$$4 \cdot 61 - 234$$

$$51 = 5 \cdot 10 + 1 \Rightarrow 1 = 51 - 5 \cdot 10 = 234 - 3 \cdot 61 - 5(4 \cdot 61 - 234) =$$

$$1 = 6 \cdot 234 - 23 \cdot 61$$

$$gcd = 1$$

דוגמא נוספת:

$$(224, 63) =?$$

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

$$(63, 35) =?$$

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

$$4 \cdot 63 - 224$$

$$(35, 28) =?$$

$$35 = 28 + 7 \Rightarrow 7 = 35 - 28 =$$

$$224 - 3 \cdot 63 - (4 \cdot 63 - 224) = 2 \cdot 224 - 7 \cdot 63$$

תזכורת: יהי $m \in N$. ו$x, y \in \mathbb{Z}$. נגיד ש$x \equiv y \mod m$ אם

$$m|(x - y)$$

לדוגמא:

$$1 \equiv 4 \mod 3$$

משפט השאריות הסיני: יהיו $(m, n) = 1$. אזי לכל $a, b \in Z$ קיים x כך ש:

$$x \equiv a \mod m$$

$$x \equiv b \mod n$$

דוגמא: $(5, 7) = 1$.

$$x \equiv 1 \mod 5$$

$$x \equiv 2 \mod 7$$

$$x = 16$$

$$x \equiv 3 \mod 5$$

$$x \equiv 4 \mod 7$$

$$x = 53$$

משפט השאריות הסיני: יהיו $(m, n) = 1$. אזי לכל $a, b \in Z$ קיים x כך ש:

$$x \equiv a \mod m$$

$$x \equiv b \mod n$$

הוכחה: קיים צירוף לינארי:

$$\alpha m + \beta n = 1, \alpha, \beta \in \mathbb{Z}$$

נקח

$$x = b\alpha m + a\beta n$$

למה זה עובד?

$$x \mod m = a\beta n \mod m = a(1 - \alpha m) \mod m = a \mod m$$

$$x \mod n = b\alpha m \mod n = b(1 - \beta n) \mod n = b \mod n$$

תרגיל: מצאו

$$x \equiv 1 \mod 3$$

$$x \equiv 2 \mod 5$$

פתרון:

$$2 \cdot 5 - 3 \cdot 3 = 1$$

$$1 \cdot 2 \cdot 5 - 2 \cdot 3 \cdot 3 = -8$$

הערה: x יחיד עד כך מודולו mn.