1. *Bizonyítsuk be a legnagyobb közös osztó következő tulajdonságait! Ne használjuk a prímfaktorizációt, csak az euklideszi algoritmust!*

(i) Ha a, b-re alkalmazzuk az euklideszi algoritmust és a maradékok $r_1, r_2, \cdots, r_n, 0$, akkor $(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n) = (r_n, 0)$.

(ii) Ha $a, b, c \in \mathbb{Z}$ és $c > 0$ akkor $(ca, cb) = c(a, b)$.

(iii) Ha $(a, b) = d$ akkor $(a/d, b/d) = 1$.

(iv) $(a + nb, b) = (a, b)$ minden n egész számra.

(v) Ha $c|ab$ és $(c, a) = 1$, akkor $c|b$. Használjuk a (iii)-at.

Megoldás: Az egyszerűség kedvéért használjuk az $r_{-1} = a$, $r_0 = b$, $r_{n+1} = 0$ jelölést.

(i) Az (r_i, r_{i+1}) párra az euklideszi algoritmus az (a, b)-re alkalmazott euklideszi algoritmus utolsó $n - i$ lépése, tehát ugyanazt az r_n-t kapjuk legnagyobb közös osztóként, mint (a, b)-re.

(ii) Ha a (ca, cb) párra alkalmazzuk az euklideszi algoritmust, akkor mindegyik maradékos osztás c-vel megszorzódik: $r_{i-2} = r_{i-1}q_i + r_i$ helyett $cr_{i-2} = cr_{i-1}q_i + cr_i$ valóban maradékos osztás, mert $0 \le r_i < |r_{i-1}|$-ből $0 \le cr_i < c|r_{i-1}| = |cr_{i-1}|$ következik. Így az első 0 maradék itt is az $(n + 1)$-edik, és az előtte levő $cr_n = c(a, b)$ a ca és cb legnagyobb közös osztója.

(iii) Használjuk a (ii) állítást: $(a, b) = d$ miatt d osztója a-nak és b-nek, így a/d és b/d egész számok. Tehát $d = (a, b) = (d(a/d), d(b/d)) = d(a/d, b/d) \Rightarrow 1 = (a/d, b/d)$.

(iv) Ha az (a, b)-re alkalmazott euklideszi algoritmus első lépése $a = bq_1 + r_1$, akkor $a + nb = b(q_1 + n) + r_1$ az $(a + nb, b)$ párra alkalmazott euklideszi algoritmus kezdő lépése, és innentől kezdve a maradékos osztások megegyeznek, így a legutolsó nem nulla maradék is ugyanaz.

(v) A (ii) miatt $(cb, ab) = (c, a)b = b$. Másrészt c osztója cb-nek és ab-nek is, azaz közös osztója cb-nek és ab-nek, tehát c osztója a legnagyobb közös osztójuknak, b-nek.

2. *(Kibővített euklideszi algoritmus) Az euklideszi algoritmus felhsználásával mutassuk meg, hogy minden a, b egész számhoz léteznek olyan α, β egész számok, hogy $\alpha a + \beta b = d$, ahol $d = (a, b)$.*

Megoldás: Belátjuk, hogy az euklideszi algoritmus minden maradéka (r_i, $i = -1, 0, \ldots, n$) előáll $\alpha a + \beta b$ alakban alkalmas $\alpha, \beta \in \mathbb{Z}$-vel. Ugyanis $r_{-1} = a = 1 \cdot a + 0 \cdot b$, $r_0 = b = 0 \cdot a + 1 \cdot b$, és tetszőleges $0 \le i \le n$-re $r_i = r_{i-2} - r_{i-1}q_i$, tehát ha $r_{i-2} = \alpha_{i-2}a + \beta_{i-2}b$ és $r_{i-1} = \alpha_{i-1}a + \beta_{i-1}b$, akkor $r_i = (\alpha_{i-2} - \alpha_{i-1}q_i)a + (\beta_{i-2} - \beta_{i-1}q_i)b$, tehát teljes indukcióval láthatjuk, hogy minden r_i, így $r_n = d$ is előáll $\alpha a + \beta b$ alakban.

3. *A 2. feladat segítségével adjunk másik bizonyítást 1.(v)-re.*

Megoldás: A 2. feladat állítása szerint van olyan $x, y \in \mathbb{Z}$, amelyre $1 = xc + ya$, így $b = xbc + yab$, de xbc és yab is osztható c-vel, ezért $c \mid b$.

4. *a) Osszuk el maradékosan 20-at és -20-at 7-tel és -7-tel.*

b) Határozzuk meg $20/7, -20/7$ felső és alsó egész részeit.

Megoldás: a)

$$\begin{aligned} 20 &= 7 \cdot 2 + 6 \\ 20 &= (-7)(-2) + 6 \\ -20 &= 7(-3) + 1 \\ -20 &= (-7)3 + 1 \end{aligned}$$

b) $\lfloor 20/7 \rfloor = 2$, $\lceil 20/7 \rceil = 3$, $\lfloor -20/7 \rfloor = -3$, $\lceil 20/7 \rceil = -2$.

5. *Határozzuk meg euklideszi algoritmussal $(288, 204)$-et és állítsuk elő a legnagyobb közös osztót egész együtthatós lineáris kombinációként.*

Megoldás:

		288	244
	288	1	0
$-1\cdot$	244	0	1
$-5\cdot$	44	1	-1
$-1\cdot$	24	-5	6
$-1\cdot$	20	6	-7
$-5\cdot$	4	-11	13
	0		

vagy rövidebben

		288	244
	288	1	0
$-1\cdot$	244	0	1
$-6\cdot$	44	1	-1
$2\cdot$	-20	-6	7
$5\cdot$	4	-11	13
	0		

(A második esetben a maradékos osztásnak a legkisebb abszolút értékű maradékot adó változatát használtuk.) Tehát $(288, 204) = 4 = -11 \cdot 288 + 13 \cdot 244$.

6. *(Diofantoszi egyenlet)*

(i) Mutassuk meg, hogy ha a, b, c egész számok, és $ax + by = c$-nek van egész (x, y) megoldása, akkor $(a, b)|c$.

(ii) Fordítva, ha $(a, b)|c$, akkor van (x, y) megoldása az egészek körében $ax + by = c$-nek.

(iii) Mutassuk meg, hogy ha (x_0, y_0) és (x', y') két megoldása $ax + by = c$-nek az egészek körében, akkor van olyan t egész szám, hogy $x' = x_0 + (b/d)t$ és $y' = y_0 - (a/d)t$. Azaz a diofantoszi egyenlet összes megoldása egy megoldása segítségével kifejezhető és minden ilyen alakú (x', y') számpár megoldása a diofantoszi egyenletnek, ha t egész és (x_0, y_0) megoldás.

Megoldás: (i) Mivel (a, b) osztója a-nak és b-nek, osztója ax-nek és by-nak is, és így osztója $ax + by = c$-nek.

(ii) A 2. feladatban láttuk, hogy van olyan (x_0, y_0), amelyre $ax_0 + by_0 = (a, b)$, és így a $k := \frac{c}{(a,b)}$ egész számmal felszorozva azt kapjuk, hogy $a(kx_0) + b(ky_0) = c$.

(iii) $ax_0 + by_0 = c = ax' + by' \Rightarrow b(y_0 - y') = a(x' - x_0) \Rightarrow$

$$(b/d)(y_0 - y') = (a/d)(x' - x_0). \tag{1}$$

De az 1.(iii) feladat szerint $(a/d, b/d) = 1$. Továbbá $(b/d) \mid (a/d)(x' - x_0)$, ezért az 1.(v) szerint $(b/d) \mid (x' - x_0)$, vagyis van olyan $t \in \mathbb{Z}$, amelyre $x' - x_0 = (b/d)t$. Ezt behelyettesítve az (1) egyenlőségbe, és egyszerűsítve (b/d)-vel, azt kapjuk, hogy $y_0 - y' = (a/d)t$. Tehát $x' = x_0 + (b/d)t$ és $y' = y_0 - (a/d)t$.

Másfelől, ha (x_0, y_0) megoldás, akkor nyilván megoldás az $x' = x_0 + (b/d)t$ és $y' = y_0 - (a/d)t$ pár is, ha t egész: $a(x_0 + (b/d)t) + b(y_0 - (a/d)t) = ax_0 + by_0 + (ab/d)t - (ab/d)t = ax_0 + by_0 = c$.

7. *Megoldhatók-e az alábbi diofantoszi egyenletek? Ha igen, adjuk meg az összes megoldásukat!*

a) $288x + 204y = 1$

b) $288x + 204y = 48$

Megoldás: a) Nem oldható meg, mert $(288, 204)$ nem osztója 1-nek (számolás nélkül is látszik, hogy a legnagyobb közös osztó 4-nek többszöröse).

b)

		288	204
	288	1	0
$-1\cdot$	204	0	1
$-2\cdot$	84	1	-1
$-2\cdot$	36	-2	3
$-3\cdot$	12	5	-7
	0		

Mivel $(288, 204) = 12 \mid 48$, a diofantoszi egyenlet megoldható, és egyik megoldását megkaphatjuk a 12 előállításának megfelelő többszöröseként: $(x_0, y_0) = (20, -28)$ (de akár a 36 és a 12 előállításának az összegeként kaphatunk egy másik megoldást: $(3, -4)$). Ebből az összes megoldás felírható: $(20 + \frac{204}{12}t,\ -28 - \frac{288}{12}t) = (20 + 17t,\ -28 - 24t)$, ahol $t \in \mathbb{Z}$ tetszőleges.

8. *a) Váltsuk át* 26*-ot* $10, 16, 8, 4, 2, 5, 26$ *alapú számrendszerbe.*
b) Váltsuk át 1001*-et* 2*-es,* 8*-as és* 16*-os számrendszerbe.*

Megoldás: a) Ismételt leosztásokkal, és a maradékok fordított sorrendben való felírásával:

10		16		8		4		2		5		26	
26	6	26	10	26	2	26	2	26	0	26	1	26	0
2	2	1	1	3	3	6	2	13	1	5	0	1	1
		0		0		1	1	6	0	1	1	0	
						0		3	1	0			
								1	1				
								0					

26 a megadott számrendszerekben:

$$26_{10} = 1A_{16} = 32_8 = 122_4 = 11010_2 = 101_5 = 10_{26}.$$

b) A b alapú számrendszerből b^m alapúba való átváltást a számjegyek csoportosításával (jobbról balra m tagú csoportokba) és a csoportok átváltásával, a b^m alapú számrendszerről b alapú számrendszerre való átváltást az egyes számjegyek átváltásával el lehet végezni, ugyanis egy a b-es számrendszerben n-jegyű c számra és $k = \lceil n/m \rceil$-re
$c = a_{n-1}b^{n-1} + a_{n-2}b^{n-2} + \ldots + a_1 b + a_0 = (a_{km-1}b^{m-1} + \ldots + a_{km-m+1}b + a_{k(m-1)})b^{(k-1)m} + \ldots + (a_{2m-1}b^{m-1} + \ldots + a_{m+1}b + a_m)b^m + (a_{m-1}b^{m-1} + a_1 b + \ldots + a_0)$, ahol $a_i := 0$, ha $i \geq n$, és itt $0 \leq a_{im-1}b^{m-1} + \ldots + a_{im-m+1}b + a_{(i-1)m} < b^m$.
Érdemes a 8-as számrendszerrel kezdeni, és abból átváltani.

8	
1001	1
125	5
15	7
1	1
0	

$1001 = 1751_8 = 1|111|101|001_2 = 11|1110|1001_2 = 3E9_{16}$.

9. *Horner-módszerrel helyettsítsük be* 5*-öt a* $p(x) = x^5 - 3x^2 + x + 3$ *polinomba.*

Megoldás:

	1	0	0	−3	1	3
5	1	5	25	122	611	3058

$\Rightarrow \qquad p(5) = 3058$

10. *Adjuk meg* 120201_3*-at tízes számrendszerben Horner módszerrel.*

Megoldás:

	1	2	0	2	0	1
3	1	5	15	47	141	424

$\Rightarrow \qquad 120201_3 = 424_{10}.$