1. *Oldjuk meg a következő lineáris kongruenciákat!*

a) $12x \equiv 15 \pmod{21}$

b) $12x \equiv 4 \pmod{2}$

Megoldás:

a)
$$\begin{aligned} 12x &\equiv 15 && \pmod{21} \\ 4x &\equiv 5 && \pmod{7} \\ 4x &\equiv 12 && \pmod{7} \\ x &\equiv 3 && \pmod{7} \\ x &\equiv 3, 10 \text{ vagy } 17 && \pmod{7} \end{aligned}$$

b)
$$\begin{aligned} 12x &\equiv 4 && \pmod{2} \\ 6x &\equiv 2 && \pmod{1} \\ x &\quad \text{bármi lehet} \\ x &\equiv 1,\ 2 && \pmod{2} \end{aligned}$$

2. *Oldjuk meg az alábbi kongruenciarendszert!*

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 4 \pmod{7} \end{aligned}$$

Megoldás:

$$\begin{aligned} x &\equiv 2 && \pmod{3} \\ x &\equiv 3 && \pmod{5} \\ x &\equiv 4 && \pmod{7} \end{aligned}$$

m_i	3	5	7
M_i	35	21	15
$x_i \equiv M_i^{-1}(m_i)$	-1	1	1
a_i	2	3	4

$x \equiv 35 \cdot (-1) \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 4 \equiv 53 \pmod{105}$.

3. *a) Határozzuk meg* $5^{-1} \bmod 26$ *értékét!*

b) Az a)-beli megoldás segítségével oldjuk meg az alábbi kongruenciát:

$$5x \equiv 7 \pmod{26}$$

c) Invertálható-e 4 *modulo* 26*?*

Megoldás: a)

$$\begin{aligned} 5x &\equiv 1 \equiv -25 \pmod{26} \\ x &\equiv -5 \equiv 21 \pmod{26} \end{aligned}$$

$$5^{-1} \bmod 26 = 21$$

b) Az a) alapján $x \equiv 7 \cdot 5^{-1} \equiv 7 \cdot (-5) \equiv -35 \equiv 17 \pmod{26}$.

c) Nem, mert $(4, 26) = 2$ nem osztója 1-nek, tehát nem lehet megoldani a $4x \equiv 1 \pmod{26}$ kongruenciát.

4. *a) Mutassuk meg, hogy* $\varphi(p) = p - 1$*, és* $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$*, ha* p *prím.*

b) Bizonyítsuk be, hogy ha p *végigfut* n *prímosztóin, akkor*

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Megoldás: a) Az $1, \ldots, p$ közül pontosan az első $p-1$ relatív prím p-hez, tehát $\varphi(p) = p-1$. Az $1, \ldots, p^\alpha$ számok közül a p^α-hoz nem relatív prímek a p-vel oszthatók, és ezek éppen a p-edrészét adják a p^α-ig terjedő pozitív egészeknek, tehát $\varphi(p^\alpha) = p^\alpha - \frac{1}{p}p^\alpha = p^\alpha - p^{\alpha-1}$.

b) Legyen $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ az n kanonikus alakja, és legyen A_i a p_i-vel nem osztható számok halmaza $\{1, \ldots, n\}$-ben. Ekkor a szitaformula szerint

$$|A_1 \cup \ldots \cup A_r| = \sum_i |A_i| - \sum_{i \neq j} |A_i \cup A_j| + \sum_{i,j,k \text{ kül.}} |A_i \cap A_j \cap A_k| - \ldots =$$

$$\sum \frac{1}{p_i} n - \sum \frac{1}{p_i p_j} n + \sum \frac{1}{p_i p_j p_k} n - \ldots,$$

és így az n-hez relatív prímek száma

$$n \cdot \left(1 - \sum \frac{1}{p_i} + \sum \frac{1}{p_i p_j} - \sum \frac{1}{p_i p_j p_k} + \ldots\right) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

5. *Készítsük el a Z_5 és Z_6 összeadás- és szorzástábláját!*
Készítsük el a mod 6 *redukált maradékosztályok szorzástábláját!*

Megoldás: $\mathbb{Z}_5$-re:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\mathbb{Z}_6$-ra:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$\mathbb{Z}_6^*$-ra:

·	1	5
1	1	5
5	5	1

6. *a) Mutassuk meg, hogy ha* $(m,n)=1$*, akkor* $(a \bmod m, b \bmod n) \to c \bmod mn$ *leképezés bijekció* $\mathbb{Z}_m \times \mathbb{Z}_n$ *és* $\mathbb{Z}_{mn}$ *között, ahol* c *megoldása az alábbi kongruencia rendszernek:*

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

b) Mutassuk meg, hogy az előző bijekció bijekciót ad a $(a \bmod m, b \bmod n)$ *redukált maradékosztálypárok és a* $\bmod mn$ *redukált maradékosztályok között is!*
c) Mutassuk meg, hogy ha $(m,n)=1$ *akkor* $\varphi(mn)=\varphi(m)\varphi(n)$*.*
d) Mutassuk meg, hogy az a)-beli leképezés kompatibilis az összeadással és a szorzással.

Megoldás: a) Legyen

$$\psi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$$
$$c \mapsto (c \bmod m,\ c \bmod n).$$

Ez a leképezés szürjektív és injektív, mert $\forall (a,b) \in \mathbb{Z}_m \times \mathbb{Z}_n$-re az

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

kongruenciarendszernek egyértelmű megoldása van modulo mn. A feladatban leírt bijekció ennek a ψ-nek az inverze.

b) Jelöljük $\mathbb{Z}_n^*$-nel a $\mathbb{Z}_n$-ben az n-hez relatív prím elemek halmazát. Ekkor $\psi\Big|_{\mathbb{Z}_{mn}^*}$ képe $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$, ugyanis minden $c \in \mathbb{Z}_{mn}$-re $(mn,c)=1 \Leftrightarrow (m,c)=1=(n,c)$, tehát ha $c \in \mathbb{Z}_{mn}^*$-re $a = c \bmod m$ és $b = c \bmod n$, akkor $(a,b) \in \mathbb{Z}_m^* \times \mathbb{Z}_n^*$. Fordítva, $\forall\ (a,b) \in \mathbb{Z}_m^* \times \mathbb{Z}_n^*$-re a feladatban megadott kongruenciarendszer c megoldására $(c,m)=(a,m)=1$ és $(c,n)=(b,n)=1$, így $(c,mn)=1$.

c) Mivel ψ injektív, b)-ből következik, hogy $\varphi(mn)=|\mathbb{Z}_{mn}^*|=|\mathbb{Z}_m^* \times \mathbb{Z}_n^*|=\varphi(m)\cdot\varphi(n)$.

d) $\varphi(c_1+c_2)=((c_1+c_2) \bmod m,\ (c_1+c_2) \bmod n)=$
$(c_1 \bmod m + c_2 \bmod n,\ c_1 \bmod n + c_2 \bmod n)=\psi(c_1)+\psi(c_2)$, ahol az összeadás $\mathbb{Z}_m$-beli, illetve $\mathbb{Z}_n$-beli. A szorzástartás ugyanígy felírható.

7. *Határozzuk meg az alábbi értékeket!:*
a) $\varphi(23),\ \varphi(8),\ \varphi(24)$
b) $7^{23} \bmod 23,\ \ 5^{\varphi(8)} \bmod 8,\ \ 5^8 \bmod 24,\ \ (21)^8 \bmod 24$

Megoldás: a) $\varphi(23)=22$, $\varphi(8)=\varphi(2^3)=(2-1)2^2=4$,
$\varphi(24)=\varphi(2^3\cdot 3)=(2-1)2^2\cdot(3-1)=8$.

b) $(7,23)=1 \Rightarrow 7^{23}=7^{22}\cdot 7 \equiv 1\cdot 7 \equiv 7 \pmod{23}$,
$(5,8)=1 \Rightarrow 5^{\varphi(8)} \equiv 1 \pmod{8}$,
$(5,24)=1 \Rightarrow 5^8=5^{\varphi(24)} \equiv 1 \pmod{24}$.
Mivel 15 nem relatív prím 24-hez, a $(15)^8$-ból csak az 5^8 részre használhatjuk az Euler–Fermat-tételt.
$(15)^8 = 3^8\cdot 5^8 \equiv 3^8\cdot 1 \equiv 9^2 \equiv 9 \pmod{24}$. (De számolhattuk volna helyette $(15)^8 \equiv (-9)^8 \pmod{24}$-et is. Mivel $9^2=81\equiv 9 \pmod{24}$, rögtön megkapjuk, hogy $(-9)^8=9^8\equiv 9 \pmod{24}$.

8. *Adjuk meg az alábbi komplex számok algebrai alakját:*

a) $(3-4i)(7+8i)$ *b)* $(3-4i)/(2-i)$ *c)* i^{2018} *d)* $(1+i)^9$

Megoldás: a) $(3-4i)(7+8i) = 53-4i$

b) $\dfrac{3-4i}{2-i} = \dfrac{(3-4i)(2+i)}{5} = 2-i$

c) $i^4 = (-1)^2 = 1$, ezért $i^{2018} = i^{2016} \cdot i^2 = 1 \cdot (-1) = -1$

d) $(1+i)^2 = 2i \Rightarrow (1+i)^9 = (2i)^4(1+i) = 2^4 i^4(1+i) = 16+16i$.

10. *Mi a mértani helye a síkon azon pontoknak, amelyeknek megfelelő z komplex számokra:*

a) $|z-5+i| = 2$ *b)* $|z-i| = |z+i|$ *c)* $|(z-3+4i)/(z-i)| \geq 1$

d) $|z| = 3iz$ *e)* $z+\overline{z} < 4$ *f)* $2z+5 = 2\overline{z}$.

Megoldás: a) $|z-5+i| = |z-(5-i)|$ a z pont távolsága az $5-i$-től, tehát az egyenlet megoldásai az $5-i$ középpontú, 2 sugarú kör pontjai.

b) Az i-től és $-i$-től azonos távolságra levő pontok halmaza az i-t és $-i$-t összekötő szakasz felező merőlegese, azaz az x tengely (valós tengely) a komplex számsíkon.

c) $|(z-(3-4i)| \geq |z-i| \Leftrightarrow z$ a $3-4i$ és i pontokat összekötő szakasz felező merőlegese által határolt zárt félsíkok közül az, amelyik az i-t tartalmazza.

d) Mivel $||z|| = |z|$, és $|3iz| = 3|z|$, az egyenlőség csak akkor teljesülhet, ha $|z| = 0$, azaz ha $z = 0$.

e) Írjuk fel a z komplex számot algebrai alakban: $z = x+yi$, ahol $x, y \in \mathbb{R}$. Ekkor az egyenlet: $x+yi+x-yi < 4$, azaz $x < 2$. Tehát a megoldáshalmaz az $x = 2$ függőleges egyenes által határolt bal oldali nyílt félsík.

f) Ismét algebrai alakba átírva az egyenletet: $2x+2yi+5 = 2x-2yi \Leftrightarrow 2x+5 = 2x$ és $y = 0$, de ennek az egyenletrendszernek nincs megoldása, így a megoldáshalmaz az üreshalmaz.