Gyakorló feladatok

1. *Bizonyítsuk be Wilson tételét:* $(p-1)! \equiv -1 \pmod{p}$ *minden* p *prímre.*

Megoldás: $p = 2$-re $1! = 1 \equiv -1 \pmod{2}$.
$p \geq 2$-re párosítsuk az $1, 2, \ldots, p-1$ számokat a mod p inverzükkel. Lesz olyan szám, aminek sajátmaga az inverze:

$$x \equiv x^{-1}\ (p) \ \Leftrightarrow\ x^2 \equiv 1\ (p) \ \Leftrightarrow\ p \mid (x^2-1) = (x-1)(x+1),$$

és ez utóbbi ekvivalens azzal, hogy $p \mid x-1$ vagy $p \mid x+1$, mivel p prím. Tehát 1-nek és $p-1$-nek önmaga az inverze, a többieknek nem. Ezért megfelelően csoportosítva a $(p-1)!$ tényezőit,

$$1 \cdot 2 \cdots (p-1) \equiv 1^{(p-3)/2} \cdot 1 \cdot (-1) \equiv -1 \pmod{p}.$$

2. *Oldjuk meg az alábbi kongruenciarendszert!*

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{8} \\ x &\equiv -4 \pmod{11} \end{aligned}$$

Megoldás:

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{8} \\ x &\equiv -4 \pmod{11} \end{aligned}$$

m_i	3	8	11
M_i	88	33	24
$x_i \equiv M_i^{-1}(m_i)$	1	1	6
a_i	2	3	-4

$$x \equiv 88 \cdot 1 \cdot 2 + 33 \cdot 1 \cdot 3 + 24 \cdot 6 \cdot (-4) = 176 + 99 - 576 = -301 \equiv -37 \pmod{264}.$$

2. *megoldás:* behelyettesítésekkel. Az első kongruencia ekvivalens azzal, hogy $x = 2 + 3y$ valamely $y \in \mathbb{Z}$-re.
Ezt behelyettestítve a másodikba:

$$2 + 3y \equiv 3\ (8) \ \Leftrightarrow\ 3y \equiv 1 \equiv 9\ (8) \ \Leftrightarrow\ y \equiv 3\ (8).$$

Az utóbbi azzal ekvivalens, hogy $y = 3 + 8z$ valamely $z \in \mathbb{Z}$-re, vagyis $x = 2 + 3(3 + 8z) = 11 + 24z$. Ezt behelyettesítve a harmadikba:

$$11 + 24z \equiv -4\ (11) \ \Leftrightarrow\ 24z \equiv -15\ (11) \ \Leftrightarrow\ 2z \equiv -4\ (11) \ \Leftrightarrow\ z \equiv -2\ (11).$$

Tehát $z = -2 + 11u$ valamely $u \in \mathbb{Z}$-re, amiből $x = 11 + 24(-2 + 11u) = -37 + 264u$, vagyis $x \equiv -37 \pmod{264}$.

3. *Határozzuk meg az alábbi értékeket:*

a) $\varphi(23)$, $\varphi(21)$, $\varphi(63)$, $\varphi(10!)$,

b) $120^{24} \bmod 23$, $115^{21} \bmod 21$, $68^{111} \bmod 63$, $111^{68} \bmod 63$. *Vigyázzunk,* 111 *nem relatív prím a* 63*-hoz!*

c) $3^{3^{3^4}}$ *utolsó két számjegye.*

Megoldás: a) $\varphi(23) = 22$, $\varphi(21) = \varphi(3 \cdot 7) = (3-1)(7-1) = 12$, $\varphi(63) = \varphi(3^2 \cdot 7) = 3(3-1)(7-1) = 36$,
10! kanonikus alakjában az egyes prímek kitevőjét a Legendre-formulával számíthatjuk ki:
$[10!]_2 = \left\lfloor \frac{10}{2} \right\rfloor + \left\lfloor \frac{10}{4} \right\rfloor + \left\lfloor \frac{10}{8} \right\rfloor = 5 + 2 + 1 = 8$,
$[10!]_3 = \left\lfloor \frac{10}{3} \right\rfloor + \left\lfloor \frac{10}{9} \right\rfloor = 4$,
$[10!]_5 = \left\lfloor \frac{10}{5} \right\rfloor = 2$, $[10!]_7 = 1$.
Tehát $\varphi(10!) = \varphi(2^8 \cdot 3^4 \cdot 5^2 \cdot 7) = 2^7(2-1)3^3(3-1)5(5-1)(7-1) = 2^7 \cdot 3^3 \cdot 2 \cdot 5 \cdot 4 \cdot 6 = 2^{11} \cdot 3^4 \cdot 5 = 829440$.

b) $120^{24} \bmod 23$:
$120 \equiv 5 \pmod{23} \Rightarrow 120^{24} \equiv 5^{24} \pmod{23}$, és $(5, 23) = 1$, ezért egyszerűsíthetjük a kitevőt is modulo $\varphi(23) = 22$.
$24 \equiv 2 \pmod{22}$, tehát $120^{24} \equiv 5^2 \equiv 25 \equiv 2 \pmod{23}$.

$115^{21} \bmod 21$:
$115 \equiv 10 \pmod{21}$, és $(10, 21) = 1$, továbbá $\varphi(21) = 12$, ezért $115^{21} \equiv 10^9 \pmod{21}$. Gyors hatványozással azt kapjuk, hogy $10^2 \equiv -5 \pmod{21}$, $10^4 \equiv 25 \equiv 4 \pmod{21}$, $10^8 \equiv 16 \equiv -5 \pmod{21}$, $10^9 \equiv -50 \equiv 13 \pmod{21}$.

$68^{111} \bmod 63$:
$(63, 68) = 1$ és $\varphi(63) = 36$, így $68^{111} \equiv 5^3 \equiv 125 \equiv 62 \pmod{63}$.

$111^{68} \bmod 63$:
63 prímosztói közül 3 osztója a hatványalapnak is, ezért a kongruenciát kettéválasztjuk:
$111^{68} \equiv x \pmod{63} \Leftrightarrow 111^{68} \equiv x \pmod{9}$ és $111^{68} \equiv x \pmod{7}$.
Mivel $3 \mid 111$, azt kapjuk, hogy $9 \mid 3^{68} \mid 111^{68}$, így $x \equiv 0 \pmod{9}$.
Modulo 7 viszont egyszerűsíthetünk: $111^{68} \equiv (-1)^2 \equiv 1 \pmod{7}$. Így csak az $x \equiv 0 \pmod{9}$ és $x \equiv 1 \pmod{7}$ kongruenciarendszer megoldását kell megtalálnunk a kínai maradéktétel algoritmusával. A megoldás
$x \equiv 7 \cdot 4 \cdot 0 + 9 \cdot 4 \cdot 1 \equiv 36 \pmod{63}$.

c) $3^{3^{3^4}} \equiv? \pmod{100}$, $(3, 100) = 1$, $\varphi(100) = 40$
$3^{3^4} \equiv? \pmod{40}$, $(3, 40) = 1$, $\varphi(40) = 16$
$3^4 = 81 \equiv 1 \pmod{16} \Rightarrow$
$3^{3^4} \equiv 3^1 \equiv 3 \pmod{40} \Rightarrow$
$3^{3^{3^4}} \equiv 3^3 \equiv 27 \pmod{100}$,
tehát a $3^{3^{3^4}}$ szám 27-re végződik.

4. *Készítsük el a $\mathbb{Z}_5$ és $\mathbb{Z}_6$ gyűrűk összeadás- és szorzástábláját!*
Készítsük el a mod 6 *redukált maradékosztályok csoportjának, $\mathbb{Z}_6^*$-nak a 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

$\cdot$	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

$\cdot$	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:

$\cdot$	1	5
1	1	5
5	5	1

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

a) $(3-4i)(7+8i)$ *b)* $(3-4i)/(2-i)$ *c)* i^{199} *d)* $(1+i)^9$

Megoldás: a) $53-4i$.

b) $\frac{(3-4i)(2+i)}{(2-i)(2+i)} = \frac{10-5i}{4+1} = 2-i$.

c) Mivel $i^4 = (-1)^2 = 1$, $i^{199} = i^3 = -i$.

d) Mivel $(1+i)^2 = 2i$, $(1+i)^9 = (2i)^4 \cdot (1+i) = 16+16i$.

6. *Legyen* $z = 1+3i$ *és* $u = 2-i$. *Számítsuk ki az alábbi kifejezések értékét:*

a) $z\bar{z}$ *b)* $u/\bar{u}$ *c)* $|z-u|$ *d)* $|2z-zu|$ *e)* $|u/z\bar{u}^3|$.

Megoldás: a) $z\bar{z} = |z|^2 = 1+9 = 10$.

b) $u/\bar{u} = u^2/(u\bar{u}) = (3-4i)/5 = \frac{3}{5} - \frac{4}{5}i$.

c) $|z-u| = |-1+4i| = \sqrt{17}$.

d) $|2z-zu| = |2-u| \cdot |z| = |i| \cdot |1+3i| = \sqrt{10}$.

e) $|u/(z\bar{u}^3)| = |u|/(|z| \cdot |\bar{u}|^3) = |u|/(|z||u|^3) = 1/(|z||u|^2) = 1/(5\sqrt{10})$.

7. *Oldjuk meg a komplex számok halmazán a*

$$z^2 + 2iz - 1 + i = 0$$

egyenletet!

Megoldás: A másodfokú egyenlet megoldóképlete szerint a gyökök $\frac{-2i \pm \sqrt{-4+4-4i}}{2} = \frac{-2i \pm \sqrt{-4i}}{2}$. Számítsuk ki algebrai alakban $-4i$ négyzetgyökeit!

$x, y \in \mathbb{R}$-re $(x+yi)^2 = (x^2-y^2)+2xyi = -4i \Leftrightarrow x^2-y^2=0$ és $2xy=-4$, amiből az $y=-\frac{2}{x}$ behelyettesítés és átszorzás után azt kapjuk, hogy $x^4-4=0$. Az $x \in \mathbb{R}$ feltétel miatt ennek csak az $x=\pm\sqrt{2}$ lesz a megoldása, amiből $x+yi = \pm\sqrt{2}(1-i)$, és így az eredeti egyenlet megoldása $z_1 = \frac{\sqrt{2}}{2} + \left(-1-\frac{\sqrt{2}}{2}\right)i$ és $z_2 = -\frac{\sqrt{2}}{2} + \left(-1+\frac{\sqrt{2}}{2}\right)i$.

8. *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)* $|z|=iz$ *f)* $z+\overline{z}<4$.

Megoldás: a) $|z-(5-i)|=2$, ha z távolsága $5-i$-től 2, tehát ez az $5-i$ körüli 2 sugarú kör.

b) z távolsága i-től és $-i$-től megegyezik, tehát z az i-t és $-i$-t összekötő szakasz felező merőlegesén, azaz az x tengelyen van. A megoldás az x tengely, azaz $\{\, z \mid \operatorname{Im} z = 0 \,\}$.

c) Az egyenlőtlenséget átírhatjuk $|z-3+4i| \geq |z-i|$ alakba, és az utóbbit azok a z komplex számok elégítik ki, amelyek i-től nincsenek távolabb, mint $3-4i$-től. Ez az i-t és $3-4i$-t összekötő szakasz felező merőlegese által kettévágott sík i-t tartalmazó zárt félsíkja, kihagyva az i pontot, mert ott a hányados nincs értelmezve.

d) Ha $|z|=3iz$, akkor $|z|=|3iz|=3|z|$. Ebből következik, hogy $|z|=0$, tehát $z=0$. A mértani hely csak az origóból áll.

e) A z szám abszolút értéke csak nemnegatív valós szám lehet, így az egyenletből következik, hogy $iz=a \in \mathbb{R}$, $a \geq 0$, tehát $z=\frac{a}{i}=-ai$. Az ilyen algebrai alakú z számok pedig valóban kielégítik az egyenletet, tehát a megoldások halmaza az y tengely negatív része az origóval együtt.

f) A $z=x+yi$ algebrai alakra a feltétel $2x<4$, azaz $x<2$. A mértani hely az $x=2$ függőleges egyenes által határolt, annak bal oldalán fekvő nyílt félsík.