

A dolgozat alatt semmilyen segédeszköz nem használható. A feladatok tetszőleges sorrendben megoldhatók. Kidolgozási idő 60 perc.

1. Bizonyítsuk be, hogy $\sum_{i=1}^n F_i^2 = F_n F_{n+1}$, ahol F_n az n -edik Fibonacci-szám ($F_1 = F_2 = 1$, $F_{n+1} = F_n + F_{n-1}$)! (3 pont)

Megoldás: Teljes indukcióval. $n = 1$ -re: $1^2 = 1 \cdot 1$. Tfh. igaz valamely n -re. Ekkor $\sum_{i=1}^{n+1} F_i^2 = \left(\sum_{i=1}^n F_i^2\right) + F_{n+1}^2 = F_n F_{n+1} + F_{n+1}^2 = F_{n+1}(F_n + F_{n+1}) = F_{n+1} F_{n+2}$, tehát $n + 1$ -re is igaz.

2. A kibővített euklideszi algoritmus segítségével keressünk olyan x és y egész számokat, amelyekre $47x + 19y = 4$. (3 pont)

Megoldás:

	47	1	0
2·	19	0	1
2·	9	1	-2
	1	-2	5

Tehát $1 = 47 \cdot (-2) + 19 \cdot 5$, amit 4-gyel szorozva $4 = 47 \cdot (-8) + 19 \cdot 20$, azaz $x = -8$ és $y = 20$ az egyik megoldás. (Az összes megoldást megkapjuk $x = -8 + 19t$ és $y = 20 - 47t$ alakban, ahol $t \in \mathbb{Z}$).

3. Adjuk meg az alábbi kongruenciarendszer összes megoldását! (3 pont)

$$x \equiv 2 \pmod{4}$$

$$x \equiv 1 \pmod{5}$$

$$x \equiv -2 \pmod{7}$$

Megoldás:

m_i	4	5	7
M_i	35	28	20
$x_i \equiv M_i^{-1} (m_i)$	-1	2	-1
a_i	2	1	-2
$M_i x_i a_i$	-70	56	40

így $\sum M_i x_i a_i = -70 + 56 + 40 = 26$, tehát a megoldás $x \equiv 26 \pmod{140}$.

4. Bontsuk fel az $f(x) = x^4 + x^3 - 2x^2 + 2$ polinomot irreducibilis polinomok szorzatára $\mathbb{Q}[x]$ -ben és $\mathbb{Z}_3[x]$ -ben! (4 pont)

Megoldás: $f(x)$ lehetséges racionális gyökei $\frac{p}{q}$, ahol $p \mid 2$ és $q \mid 1$, tehát $\frac{p}{q} = \pm 1, \pm 2$. Ezek közül -1 valóban gyök, és az $x + 1$ kiemelésével:

	1	1	-2	0	2
-1	1	0	-2	2	0

azt kapjuk, hogy $f(x) = (x+1)(x^3 - 2x + 2)$, ahol a második tényező is irreducibilis a Schönemann–Eisenstein-kritérium miatt $p = 2$ -vel (de mivel csak harmadfokú, azt is elég ellenőrizni, hogy nincs racionális gyöke: ennek már $\pm 1, \pm 2$ egyike sem gyöke).

Az $f(x) = (x+1)(x^3 - 2x + 2)$ felbontás $\mathbb{Z}_3[x]$ -re is átmegy, csak azt kell megnézni, hogy a harmadfokú tényezőnek van-e gyöke \mathbb{Z}_3 -ban. $0, 1, 2$ közül a 2 gyöke: \mathbb{Z}_3 -ban $2^3 - 2 \cdot 2 + 2 = 6 = 0$, tehát $x - 2 = x + 1$ -et még egyszer ki lehet emelni $f(x)$ -ből:

$$\begin{array}{c|c|c|c|c} & 1 & 0 & -2 & 2 \\ \hline 2 & 1 & 2 & 2 & 6 = 0 \end{array}$$

Így $f(x) = (x+1)^2(x^2 + 2x + 2)$, és a másodfokú tényezőnek már nincs gyöke \mathbb{Z}_3 -ban, tehát ez irreducibilisekre bontás.

5. Határozzuk meg $-i$ köbgyökeit, és döntsük el mindegyikről, hogy hányadrendű, azaz hányadik primitív egységgyök! (4 pont)

Megoldás: $-i = \cos \frac{3\pi}{2} + i \sin \frac{3\pi}{2}$, ezért $\sqrt[3]{-i} = \cos(\frac{\pi}{2} + k \cdot \frac{2\pi}{3}) + i \sin(\frac{\pi}{2} + k \cdot \frac{2\pi}{3})$, ahol $k = 0, 1, 2$.

A köbgyökök 1 abszolút értékűek, és a szögek a 2π racionális többszörösei, tehát ezek a komplex számok véges rendűek, és a rendjüket az határozza meg, hogy a 2π -t a szögbe szorzó racionális számnak mi a nevezője az egyszerűsített alakjában (azaz mi az a legkisebb pozitív egész, amellyel beszorozva a szöget, a 2π egész számú többszörösét kapjuk). A három szög:

$$\frac{\pi}{2} = \frac{1}{4} \cdot 2\pi$$

$$\frac{\pi}{2} + \frac{2\pi}{3} = (\frac{1}{4} + \frac{1}{3})2\pi = \frac{7}{12} \cdot 2\pi, \text{ és}$$

$$\frac{\pi}{2} + \frac{4\pi}{3} = (\frac{1}{4} + \frac{2}{3})2\pi = \frac{11}{12} \cdot 2\pi,$$

tehát a három köbgyök rendje 4, 12 és 12.

6. A p prím hányadik hatványával osztható a $\binom{p^n}{p}$ binomiális együttható? (3 pont)

1. *megoldás:* $n \geq 1$ -re $\binom{p^n}{p} = \frac{p^n(p^n - 1)(p^n - 2) \cdots (p^n - (p - 1))}{p(p - 1)(p - 2) \cdots 1}$.

A számlálóban és a nevezőben is csak az első tényező osztható p -vel, mert $1 \leq k \leq p - 1$ -re p nyilván nem osztója k -nak, és mivel p^n -nek viszont osztója, ezért a $p^n - k$ számot sem osztja. Tehát a számláló pontosan p^n -nel osztható, a nevező p -vel, a hányados pedig p^{n-1} -gyel. (Ha $n = 0$, akkor a binomiális együttható $\binom{1}{p} = 0$, és ez p akárhányadik hatványával is osztható.)

2. *megoldás:* Ha $n \in \mathbb{N}^+$, akkor a $\binom{p^n}{p} = \frac{(p^n)!}{p!(p^n - p)!}$ formula és a faktoriálisokra vonatkozó Legendre-formula alkalmazásával is eredményre jutunk (bár körülményesebben):

faktoriális	p hányadik hatványával osztható
$(p^n)!$	$\left\lfloor \frac{p^n}{p} \right\rfloor + \left\lfloor \frac{p^n}{p^2} \right\rfloor + \dots + \left\lfloor \frac{p^n}{p^{n-1}} \right\rfloor + \left\lfloor \frac{p^n}{p^n} \right\rfloor = p^{n-1} + p^{n-2} + \dots + p + 1$
$p!$	$\left\lfloor \frac{p}{p} \right\rfloor = 1$
$(p^n - p)!$	$\left\lfloor \frac{p^n - p}{p} \right\rfloor + \left\lfloor \frac{p^n - p}{p^2} \right\rfloor + \dots + \left\lfloor \frac{p^n - p}{p^{n-1}} \right\rfloor = (p^{n-1} - 1) + (p^{n-2} - 1) + \dots + (p - 1) = p^{n-1} + p^{n-2} + \dots + p - n + 1$

Mivel $(p^{n-1} + p^{n-2} + \dots + p + 1) - 1 - (p^{n-1} + p^{n-2} + \dots + p - n + 1) = n - 1$, ezért p^{n-1} -gyel osztható a binomiális együttható.