Bevezetés a számításelméletbe I.
Zárthelyi feladatok
2019. október 25.

1. Az n pozitív egész utolsó két számjegye a 4-es és az 5-ös számrendszerben is 11. Mi n utolsó két számjegye a 10-es számrendszerben?

2. Mutassuk meg, hogy $1010^{1343} - 2$ osztható 2019-cel. (2019 prímtényezős felbontása: $2019 = 3 \cdot 673$.)

3. Az előadáson tanult megfelelő algoritmus alkalmazásával határozzuk meg 10^{70} maradékát 46-tal osztva. (A feladat tehát nem csupán az osztási maradék meghatározása, hanem a tanult algoritmus által végzett számítások dokumentálása is.)

4. Az $\frac{x-11}{2} = \frac{z+19}{-5}$, $y = -1$ egyenletrendszerű e egyenes ugyanabban a pontban döfi a $2x + y - 2z = 3$ egyenletű síkot, mint a $P(15, 2, -8)$ ponton átmenő f egyenes. Írjuk fel az f egyenletrendszerét.

5. Legyenek $\underline{u}$, $\underline{v}$ és $\underline{w}$ az alábbi $\mathbb{R}^4$-beli vektorok. Adjuk meg az $\langle \underline{u}, \underline{v}, \underline{w} \rangle$ generált altér összes olyan elemét, amelynek mind a négy koordinátája egyenlő.

$$\underline{u} = \begin{pmatrix} 1 \\ 2 \\ 0 \\ 0 \end{pmatrix}, \ \underline{v} = \begin{pmatrix} 1 \\ 0 \\ 3 \\ 0 \end{pmatrix}, \ \underline{w} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 4 \end{pmatrix}.$$

6*. Hány olyan b egész létezik 2 és 2019 között, amelyre létezik két olyan szomszédos pozitív egész szám, hogy mindkettőnek a b alapú számrendszerbeli számjegyeinek az összege osztható 2019-cel?

A dolgozatra kérjük jól olvashatóan felírni a következő adatokat: név, Neptun-kód, Neptun szerinti gyakorlatvezető neve.

Minden feladat 10 pontot ér, a munkaidő 90 perc. Az aláírás feltétele: a két zárthelyin átlagosan legalább 24 pont és mindkét zárthelyin külön-külön legalább 18 pont elérése. A 100%-os eredményhez elegendő 50 pontot elérni a 60-ból, az összpontszám 50 pont feletti részét IMSc pontként könyveljük el.

A feladatok megoldását indokolni kell, puszta eredményközlésért nem jár pont. A dolgozat megírása közben számológép (vagy más segédeszköz) nem használható.

Bevezetés a számításelméletbe I.
Zárthelyi feladatok — pontozási útmutató
2019. október 25.

Általános alapelvek.

A pontozási útmutató célja, hogy a javítók a dolgozatokat egységesen értékeljék. Ezért az útmutató minden feladat (legalább egy lehetséges) megoldásának főbb gondolatait és az ezekhez rendelt részpontszámokat közli. Az útmutatónak *nem célja* a feladatok teljes értékű megoldásának részletes leírása; a leírt lépések egy maximális pontszámot érő megoldás vázlatának tekinthetők.

Az útmutatóban feltüntetett részpontszámok csak akkor járnak a megoldónak, ha a kapcsolódó gondolat egy áttekinthető, világosan leírt és megindokolt megoldás egy lépéseként szerepel a dolgozatban. Így például az anyagban szereplő ismeretek, definíciók, tételek puszta leírása azok alkalmazása nélkül nem ér pontot (még akkor sem, ha egyébként valamelyik leírt tény a megoldásban valóban szerephez jut). Annak mérlegelése, hogy az útmutatóban feltüntetett pontszám a fentiek figyelembevételével a megoldónak (részben vagy egészében) jár-e, teljes mértékben a javító hatásköre.

Részpontszám jár minden olyan ötletért, részmegoldásért, amelyből a dolgozatban leírt gondolatmenet alkalmas kiegészítésével a feladat hibátlan megoldása volna kapható. Ha egy megoldó egy feladatra több, egymástól lényegesen különböző megoldást is elkezd, akkor legföljebb az egyikre adható pontszám. Ha mindegyik leírt megoldás vagy megoldásrészlet helyes vagy helyessé kiegészíthető, akkor a legtöbb részpontot érő megoldáskezdeményt értékeljük. Ha azonban több megoldási kísérlet között van helyes és (lényeges) hibát tartalmazó is, továbbá a dolgozatból nem derül ki, hogy a megoldó melyiket tartotta helyesnek, akkor a kevesebb pontot érő megoldáskezdeményt értékeljük (akkor is, ha ez a pontszám 0).

Az útmutatóban szereplő részpontszámok szükség esetén tovább is oszthatók. Az útmutatóban leírttól eltérő jó megoldás természetesen maximális pontot ér.

1. Az n pozitív egész utolsó két számjegye a 4-es és az 5-ös számrendszerben is 11. Mi n utolsó két számjegye a 10-es számrendszerben?

* * * * *

A feladat feltételeiből $n \equiv 5 \pmod{16}$ és $n \equiv 6 \pmod{25}$ adódik. (1 pont)
A kapott kongruenciarendszert a tanult módszerrel oldjuk meg.
Az első kongruenciából: $n = 16k + 5$ valamely k egészre. (1 pont)
Ezt a másodikba helyettesítve: $16k + 5 \equiv 6 \pmod{25}$. Mindkét oldalból 5-öt levonva a $16k \equiv 1 \pmod{25}$ lineáris kongruenciát kapjuk. (1 pont)
$1 \equiv -24 \pmod{25}$ miatt ez a $16k \equiv -24 \pmod{25}$ alakba írható. 8-cal osztva: $2k \equiv -3 \pmod{25}$, ahol a modulus $(8, 25) = 1$ miatt nem változott. (2 pont)
Hasonlóan folytatva: $-3 \equiv 22 \pmod{25}$ miatt a $2k \equiv 22 \pmod{25}$ alakot kapjuk. Ezt 2-vel osztva: $k \equiv 11 \pmod{25}$, ahol a modulus $(2, 25) = 1$ miatt megint nem változott. (1 pont)
Mivel mindkét megtett lépésünk ekvivalens átalakítás volt, ezért $k \equiv 11 \pmod{25}$ valóban a lineáris kongruencia megoldáshalmazát adja meg. (1 pont)
Ebből tehát $k = 25\ell + 11$ valamely ℓ egészre. Ezt visszahelyettesítve: $n = 16k + 5 = 16(25\ell + 11) + 5 = 400\ell + 181$. (2 pont)
Következik, hogy n 100-as maradéka – és így az utolsó két számjegye is –: 81. (1 pont)
A feladat valamivel kevesebb számolással is megoldható, ha az $n \equiv 5 \pmod{16}$ kongruencia helyett annak csak az $n \equiv 1 \pmod{4}$ következményét használjuk és az így kapott kongruenciarendszert oldjuk meg. A megoldás során előállt lineáris kongruencia természetesen más tanult módszerekkel, így akár az Euklideszi algoritmussal is megoldható. Aki a fent leírthoz hasonló utat választ, az a lépések ekvivalenciájára való hivatkozást kiválthatja azzal, hogy a megoldások száma előre tudhatóan 1 lesz, mert az ismeretlen együtthatója a modulushoz relatív prím; azonban a két észrevétel közül legalább az egyik szükséges a hiánytalan indokláshoz.

2. Mutassuk meg, hogy $1010^{1343} - 2$ osztható 2019-cel. (2019 prímtényezős felbontása: $2019 = 3 \cdot 673$.)

* * * * *

$(1010, 2019) = 1$ (mert 1010 se 3-mal, se 673-mal nem osztható). (1 pont)
$\varphi(2019) = \varphi(3 \cdot 673) = (3-1)(673-1) = 1344$ a tanult képlet szerint. (1 pont)
Így az Euler-Fermat tételből $1010^{1344} \equiv 1 \pmod{2019}$ következik. (2 pont)
Ez $1 \equiv 2020 \pmod{2019}$ miatt így is írható: $1010^{1344} \equiv 2020 \pmod{2019}$. (1 pont)
Mindkét oldalt 1010-zel osztva: $1010^{1343} \equiv 2 \pmod{2019}$, (2 pont)
ahol a modulus $(1010, 2019) = 1$ miatt nem változott. (1 pont)
Ebből tehát $2019 \mid 1010^{1344} - 2$ következik, ami épp a bizonyítandó állítás. (2 pont)
A megoldás második része helyettesíthető azzal is, hogy az $1010x \equiv 1 \pmod{2019}$ lineáris kongruenciának megoldása egyrészt $x = 2$ (mert $2 \cdot 1010 = 2020$), másrészt az Euler-Fermat tétel miatt $x = 1010^{1343}$ is, viszont $(1010, 2019) = 1$ miatt ennek a lineáris kongruenciának a tanult tétel szerint csak egyetlen megoldása van modulo 2019, ezért $1010^{1343} \equiv 2 \pmod{2019}$ valóban következik.

3. Az előadáson tanult megfelelő algoritmus alkalmazásával határozzuk meg 10^{70} maradékát 46-tal osztva. (A feladat tehát nem csupán az osztási maradék meghatározása, hanem a tanult algoritmus által végzett számítások dokumentálása is.)

* * * * *

A tanultak szerint ismételt négyzetre emelésekkel és a kapott eredmények 46-os maradékának meghatározásával kiszámítjuk a $10^1, 10^2, 10^4, \ldots, 10^{64}$ hatványok 46-os maradékát. Ezek sorra: 10, 8, 18, 2, 4, 16 és 26. (4 pont)
Mivel $70 = 2 + 4 + 64$, (2 pont)
ezért meghatározzuk először a $10^6 = 10^2 \cdot 10^4$, majd a $10^{70} = 10^6 \cdot 10^{64}$ hatványok 46-os maradékait a korábban kiszámolt megfelelő maradékokkal való szorzással és a kapott eredmények 46-os maradékának meghatározásával. Ezek sorra: 6 és 18. (4 pont)
Így a keresett maradék: 18.
A teljes értékű megoldáshoz nem szükséges a fenti részletességgel leírni az elvégzett műveletek mögötti szándékot, elegendő a helyes számítások közlése. Nem jelent pontlevonást, ha egy megoldó a végeredményhez először $10^{68} = 10^{64} \cdot 10^4$, majd 10^{70} maradékait határozza meg a fentihez hasonló módon. Ha viszont egy megoldó a kapott részeredményeit nem helyettesíti azok 46-os maradékaival és például 10^4 maradékához közvetlenül 10000-et osztja 46-tal, az lényeges elvi hibának számít, ami az algoritmus ismeretének alapvető hiányát mutatja; egy ilyen megoldó legföljebb 5 pontot kaphat (azt is csak akkor, ha a további számolásai hasznosak és a helyes végeredményt megkapja).

4. Írjuk fel az e egyenes egyenletrendszerét, ha tudjuk róla, hogy áthalad a $P(15, 2, -8)$ ponton és hogy e ugyanabban a pontban döfi a $2x + y - 2z = 3$ egyenletű síkot, mint az $\frac{x-11}{2} = \frac{z+19}{-5}$, $y = -1$ egyenletrendszerű f egyenes.

* * * * *

Először meghatározzuk a $2x + y - 2z = 3$ egyenletű S sík és az f egyenes Q metszéspontját. Ehhez megoldjuk az S egyenletéből és az f egyenletrendszeréből álló egyenletrendszert. (1 pont)
Az f-et leíró első egyenletből: $2z = 17 - 5x$. Ezt, illetve az $y = -1$ egyenletet az S egyenletébe helyettesítve: $2x - 1 - (17 - 5x) = 3$. Ebből $x = 3$ adódik, amiből $z = \frac{17-5\cdot3}{2} = 1$. Így a metszéspont: $Q(3; -1; 1)$ (3 pont)
Az e tehát átmegy P-n és Q-n, így irányvektora a $\overrightarrow{QP}$ vektor. (2 pont)
A P-be, illetve Q-ba mutató helyvektorokat $\underline{p}$-vel, illetve $\underline{q}$-val jelölve $\overrightarrow{QP} = \underline{p} - \underline{q} = (15; 2; -8) - (3; -1; 1) = (12; 3; -9)$. (1 pont)
(Ehelyett használhatjuk irányvektornak például a $\overrightarrow{QP}$ harmadát is, a $\underline{v}(4; 1; -3)$ vektort.)
Így az e egyenletrendszerét a $\underline{v}$ és (például) a P segítségével felírva: $\frac{x-15}{4} = y - 2 = \frac{z+8}{-3}$. (3 pont)

5. Legyenek $\underline{u}$, $\underline{v}$ és $\underline{w}$ az alábbi $\mathbb{R}^4$-beli vektorok. Adjuk meg az $\langle \underline{u}, \underline{v}, \underline{w} \rangle$ generált altér összes olyan elemét, amelynek mind a négy koordinátája egyenlő.

$$\underline{u} = \begin{pmatrix} 1 \\ 2 \\ 0 \\ 0 \end{pmatrix}, \ \underline{v} = \begin{pmatrix} 1 \\ 0 \\ 3 \\ 0 \end{pmatrix}, \ \underline{w} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 4 \end{pmatrix}.$$

* * * * *

Az $\underline{a} = \begin{pmatrix} p \\ p \\ p \\ p \end{pmatrix}$ vektor pontosan akkor van az $\langle \underline{u}, \underline{v}, \underline{w} \rangle$ generált altérben, ha $\underline{a}$ kifejezhető $\underline{u}$-ból, $\underline{v}$-ből és $\underline{w}$-ből lineáris kombinációval; vagyis ha léteznek olyan α, β, γ skalárok, hogy $\alpha \cdot \underline{u} + \beta \cdot \underline{v} + \gamma \cdot \underline{w} = \underline{a}$.(1 pont)
Behelyettesítve $\underline{u}, \underline{v}, \underline{w}$ konkrét értékét és elvégezve a műveleteket a következő lineáris egyenletrendszerre jutunk:

$$\begin{aligned} \alpha + \beta + \gamma &= p \\ 2\alpha &= p \\ 3\beta &= p \\ 4\gamma &= p \end{aligned}$$ (4 pont)

Az utolsó három egyenletből $\alpha = \frac{p}{2}$, $\beta = \frac{p}{3}$, $\gamma = \frac{p}{4}$ adódik. Ezeket az elsőbe helyettesítve $\frac{13}{12}p = p$, vagyis $p = 0$ következik. (2 pont)
Azt kaptuk tehát, hogy az $\langle \underline{u}, \underline{v}, \underline{w} \rangle$ generált altérnek a nullvektor az egyetlen olyan eleme, amelynek mind a négy koordinátája egyenlő. (3 pont)

6*. Hány olyan b egész létezik 2 és 2019 között, amelyre létezik két olyan szomszédos pozitív egész szám, hogy mindkettőnek a b alapú számrendszerbeli számjegyeinek az összege osztható 2019-cel?

* * * * *

Az alábbi megoldásban a számok számjegyeit végig b alapú számrendszerben értjük, így ezek 0 és $b-1$ közti egészek. Az n számjegyeinek az összegét pedig S_n-nel jelöljük (b alapú számrendszerben).
Tegyük fel, hogy az n és az $n+1$ pozitív egészekre S_n és S_{n+1} is osztható 2019-cel. Ekkor n utolsó jegye $b-1$ kell legyen. Ha ugyanis nem az volna, akkor $n+1$ utolsó számjegye 1-gyel volna nagyobb n-énél, a többi jegyük pedig azonos volna; így $S_{n+1} = S_n + 1$ teljesülne, ezért nem lehetne mindkettő osztható 2019-cel. (1 pont)
Jelöljük t-vel azt, hogy n hány darab $(b-1)$-es számjegyre végződik. Ekkor $n+1$ utolsó t darab jegye nyilván 0, jobbról a $(t+1)$-edik jegye 1-gyel nagyobb n-énél, a többi jegyük pedig azonos. (Ha esetleg n összesen t jegyű, akkor az előző mondatot úgy értjük, hogy az $(n+1)$-nek a jobbról $(t+1)$-edik jegye „0-ról 1-re változott" – vagyis a jegyeinek a száma 1-gyel nagyobb n-énél.) (1 pont)
Ebből tehát $S_{n+1} = S_n - (b-1) \cdot t + 1$ következik. (2 pont)
Mivel $2019 \mid S_n$ és $2019 \mid S_{n+1}$, ezért ebből az egyenletből $2019 \mid 1 - (b-1) \cdot t$, vagyis $(b-1) \cdot t \equiv 1 \pmod{2019}$ következik. (1 pont)
Ebből a lineáris kongruenciák megoldhatóságára tanult tételből $(b-1, 2019) \mid 1$, vagyis $(b-1, 2019) = 1$ következik (hiszen $x = t$ megoldása a $(b-1) \cdot x \equiv 1 \pmod{2019}$ lineáris kongruenciának). (2 pont)
Megmutattuk tehát, hogy ha léteznek a feladat szerinti n és $n+1$ egészek, akkor $(b-1, 2019) = 1$. Azonban ennek a megfordítása is igaz: valóban, ha $(b-1, 2019) = 1$, akkor a tanult tétel szerint megoldható a $(b-1) \cdot x \equiv 1 \pmod{2019}$ lineáris kongruencia, így t-nek választhatjuk ennek egy (pozitív) megoldását. Ebből n-et konstruálhatjuk úgy, hogy az utolsó t darab jegye $b-1$, majd ezek elé felveszünk néhány további számjegyet (például $2019 - ((b-1) \cdot t \bmod 2019)$ darab 1-est) úgy, hogy $2019 \mid S_n$ teljesüljön. Ekkor a fent megmutatott $S_{n+1} = S_n - (b-1) \cdot t + 1$ egyenlet miatt $2019 \mid S_{n+1}$ is igaz lesz. (2 pont)
A feladat kérdésének megválaszolásához tehát azon b egészeket kell megszámolni 2 és 2019 között, amelyekre $(b-1, 2019) = 1$. Ezeknek a száma pedig nyilván $\varphi(2019) = (3-1)(673-1) = 1344$.(1 pont)