Material Pergaditor nga Teoria e Numrave

Leart Ajvazaj

Dhjetor 2022

> Matematika është mbretëresha e të gjithë shkencave - dhe teoria e numrave është mbretëresha e matematikës
>
> C.F. Gauss

Njëra nga katër fushat kryesore në olimpiada matematike, teoria e numrave konsiderohet nga shumë si disiplina më e vjetër në matematike. Thënë me pak fjalë, teoria e numrave merret me studimin e numrave të plotë dhe numrave të thjeshtë. Bashkësia e numrave të plotë shënohet me $\mathbb{Z}$ dhe përmban

$$\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

Qëllimi i këtij materiali është paisja e nxënësve me njohuri të mjaftueshme për të kuptuar dhe zgjidhur problemet e nivelit 1/4 në olimpiadën ndërkombëtare të matematikës. Nëse vëreni probleme me këtë material, ju lutem më kontaktoni në ajvazaj.leart@gmail.com.

1 Moduli I - Plotpjesëtueshmëria

1.1 Plotpjesëtueshmëria

Njëra nga idetë më të rëndësishme në teorinë e numrave është ajo e plotpjesëtueshmërisë. Në shkollë fillore mësojmë operacionin e pjesëtimit duke vendosur theks të veçantë në rastet kur mbetja nga pjesëtimi i një numri me një tjetër është zero. Në këto raste kemi të bëjmë me plotpjesëtueshmëri.

Definicion 1.1. Le të jenë a dhe b numra të plotë dhe $a \neq 0$. Themi se a **ndanë** b (ose b është i **plotpjesëtueshëm** me a), shënuar si $a \mid b$, nëse ekziston një numër i plotë c ashtu që $b = a \cdot c$. Mund ta shohim kushtin $a \mid b$ si $\dfrac{b}{a} \in \mathbb{N}$.

Shembuj:

- $3 \mid 15$ (3 ndanë 15) meqë $15 = 3 \cdot 5$.
- $1 \mid n$ për çdo $n \in \mathbb{Z}$ pasi $n = 1 \cdot n$.

- $3 \mid -6$ pasi $-6 = 3 \cdot (-2)$
- 7 nuk e ndanë 80 (shënohet $7 \nmid 80$)

Nëse $a \mid b$ themi se a është **faktor** i b dhe b është **shumëfish** i a. Vërejmë që shumëfishët e një numri të plotë n janë $0, \pm n, \pm 2n, \pm 3n, \ldots$ Pra për n numra të njëpasnjëshëm gjithmonë ekziston një shumëfish i n. Në vijim, do të tregojmë disa veti të plotpjesëtueshmërisë.

Teoremë 1

Le të jenë a, b, c, m dhe n numra të plotë dhe le të jetë $a \neq 0$. Nëse $a \mid b$ dhe $a \mid c$, vërtetoni që $a \mid mb + nc$.

Vërtetim. Pasi $a \mid b$ dhe $a \mid c$ nga definicioni i plotpjesëtueshmërisë fitojmë $b = ax$ dhe $c = ay$ ku x dhe y janë numra të plotë. Pra

$$mb + nc = max + nay = a \cdot (mx + ny)$$

që nga definicioni do të implikon që $a \mid mb + nc$. $\square$

Teoremë 2: Tranzitiviteti i Plotpjesëtueshmërisë

Le të jenë a, b dhe c numra të plotë me $a, b \neq 0$. Nëse $a \mid b$ dhe $b \mid c$, atëherë $a \mid c$.

Vërtetim. Meqë $a \mid b$ dhe $b \mid c$, kemi $b = ax$ dhe $c = by$ ku x dhe y janë numra të plotë. Pra

$$c = by = axy = a \cdot (xy)$$

që do të thotë se $a \mid c$. $\square$

Së bashku me definicionin e parë, mund ti përdorim këto dy veti për të zgjidhur disa probleme.

Ushtrim 1.1. Gjeni të gjithë numrat natyrorë n të tillë që $n + 1 \mid n^2 + 1$.

Zgjidhje. Vërejmë që teorema 1 na tregon që nëse mbledhim (ose zbresim) dy shumëfishë të një numri, shuma (dhe ndryshimi) i tyre do të jetë shumëfish i atij numri. Pra përdorim teoremën 1 si vijon. Nëse $n + 1 \mid n^2 + 1$ atëherë kemi $n + 1 \mid n^2 + 1 - (n - 1)(n + 1)$ meqë $n + 1 \mid (n + 1)(n - 1)$. Pra kemi $n + 1 \mid 2$. Faktorët e vetëm të 2 janë $\{1, -1, 2, -2\}$ pra kemi këto mundësi:

$$n + 1 = 1 \Rightarrow n = 0. \; 0 + 1 \mid 0^2 + 1.$$
$$n + 1 = -1 \Rightarrow n = -2. \; -2 + 1 \mid (-2)^2 + 1.$$
$$n + 1 = 2 \Rightarrow n = 1. \; 1 + 1 \mid 1^2 + 1.$$
$$n + 1 = -2 \Rightarrow n = -3. \; -3 + 1 \mid (-3)^2 + 1.$$

Pra vlerat e vetme të n që plotësojnë $n + 1 \mid n^2 + 1$ janë $\{-3, -2, 0, 1\}$. $\square$

Ushtrim 1.2. Nëse $17 \mid (3x+2)$, tregoni që $17 \mid (3x^2 - x - 2)$.

Zgjidhje. Vërejmë që $3x^2 - x - 2 = (3x+2)(x-1)$. Pra mjafton të tregojmë që $17 \mid (3x+2)(x-1)$. Kjo vlen nga kushti i problemit $17 \mid 3x+2$ dhe teorema 2. $\square$

Ushtrim 1.3. Vërtetoni që $6 \mid n^3 - n$ për çdo $n \in \mathbb{N}$.

Zgjidhje. Faktorizojmë $n^3 - n$ dhe kemi $n^3 - n = n(n^2 - 1) = n(n-1)(n+1)$. Pra $n^3 - n$ është prodhimi i tre numrave të njëpasnjëshëm. Nga tre numra të njëpasnjëshëm saktësisht njëri është shumëfish i 3. Nga dy numra të njëpasnjëshëm saktësisht njëri është çift. Pra $3 \mid (n-1)n(n+1)$ dhe $2 \mid (n-1)n(n+1)$. Kemi që $(n-1)n(n+1)$ është shumëfish i 2 dhe i 3 pra $\dfrac{(n-1)n(n+1)}{2}$ dhe $\dfrac{(n-1)n(n+1)}{3}$ janë numra të plotë. Kjo implikon që ndryshimi i tyre është numër i plotë. Pra $\dfrac{(n-1)n(n+1)}{2} - \dfrac{(n-1)n(n+1)}{3} = \dfrac{(n-1)n(n+1)}{6} \in \mathbb{N}$ që implikon $6 \mid (n-1)n(n+1)$. $\square$

Shënim

Së shpejti do të kemi mundësi që nga $2 \mid a$ dhe $3 \mid a$ të konkludojmë që $6 \mid a$ pa pasur nevojë për të konsideruar ndryshimin $\dfrac{a}{2} - \dfrac{a}{3}$. Për këtë na duhet të prezantojmë numrat e thjeshtë.

Në vijim janë disa veti të tjera të rëndësishme. Nënësit inkurajohen të provojnë ti vërtetojnë këto veti.

Teoremë 3

Le të jenë a,b dhe c numra të plotë. Atëherë kemi:

(a) Nëse $a \mid b$ dhe $b \neq 0$, atëherë $|a| \leq |b|$

(b) Nëse $a \mid b$ dhe $b \mid a$, atëherë $|a| = |b|$.

(c) Nëse $a \mid b$ dhe $b \neq 0$, atëherë $\frac{b}{a} \mid b$

(d) Nëse $c \neq 0$, $a \mid b$ atëherë dhe vetëm atëherë kur $ac \mid bc$.

Vërtetim.

(a) Nëse $a \mid b$ kemi $ak = b$ për ndonjë $k \in \mathbb{Z}$. Meqë $b \neq 0$ kemi $|b| = |ka| = |k| \cdot |a|$. Pasi $k \neq 0$ kemi $|k| \geq 1$ pra $|k| \cdot |a| \geq |a|$. Rrjedhimisht, $|a| \leq |b|$.

(b) Nëse $a \mid b$ kemi $ak = b$ për ndonjë $k \in \mathbb{Z}$. Në anën tjetër, $b \mid a$ implikon që $bk' = a$ për ndonjë $k' \in \mathbb{Z}$. Duke kombinuar këto dy relacione kemi

$$a = bk' = (ak)k' = akk'.$$

Pra detyrimisht kemi $kk' = 1$. Rrjedhimisht $k = \pm 1$, qe implikon $|a| = |b|$.

(c) Meqë $a \mid b$ kemi $\frac{b}{a} \in \mathbb{Z}$. Pasi $\frac{b}{a} \cdot a = b$ kemi edhe $\frac{b}{a} \mid b$.

(b) Nëse $a \mid b$ kemi $b = ka$ pra $bc = k(ac)$ që implikon $ac \mid bc$. Në anën tjetër $ac \mid bc$ implikon $bc = kac$. Meqë $c \neq 0$ mund të pjesëtojmë të dy anët e barazimit me c dhe fitojmë $b = ka$ pra $a \mid b$.

□

Ushtrim 1.4. Tregoni që $6 \mid a + b + c \iff 6 \mid a^3 + b^3 + c^3$.

Zgjidhje. Nga njëri nga problemet paraprake kemi $6 \mid a^3 - a$, $6 \mid b^3 - b$ dhe $6 \mid c^3 - c$. Nga teorema 1 kemi $6 \mid a^3 - a + b^3 - b + c^3 - c$ pra $6 \mid (a^3 + b^3 + c^3) - (a + b + c)$. Do të thotë $6 \mid a^3 + b^3 + c^3 \iff 6 \mid a + b + c$. □

Problemet

Problem 1.1. Nëse $a^2b + a \mid b^3 + a^2b^2 + ab - a$, tregoni që $a^2b + a \mid a^2 + b^2$.

Problem 1.2. Tregoni që $6 \mid n^3 + 5n$.

Problem 1.3. Nëse $4ab - 1 \mid (4a^2 - 1)^2$, tregoni që $4ab - 1 \mid (a - b)^2$.

Problem 1.4. Nëse $5 \mid a + 2$ tregoni që $5 \mid n^2 - 4$, $5 \mid n^2 + 8n + 7$ dhe $5 \mid n^4 - 1$.

Problem 1.5. (OMK 2016 - Klasa 9). Vërtetoni që $31 \mid 5 + 5^2 + 5^3 + ... + 5^{2016}$.

Problem 1.6. Nëse $a - c \mid ab + cd$, atëherë $a - c \mid ad + bc$.

Problem 1.7. Gjeni numrin më të madh të plotë n për të cilin $n + 10 \mid n^3 + 100$

Problem 1.8. Tregoni që nëse m dhe n janë numra natyrorë të tillë që $mn \mid m^2 + n^2$, atëherë $m = n$.

Problem 1.9. (KAMO 2022 Klasa 7-8) Gjeni të gjitha dyshet e plota (m, n) ashtu që

$$m + n = 3(mn + 10).$$

1.2 Pjesëtuesi më i Madh i Përbashkët dhe Algoritmi i Euklidit

Teoremë 4: Algoritmi i Pjesëtimit

Për çdo dy numra natyrorë a, b ekziston një dyshe unike e numrave të plotë jo-negativ q, r ashtu që $a = b \cdot q + r$ ku $0 \leq r < b$.

Definicion 1.2. Le të jenë a dhe b numra të plotë, jo të dy zero. Le të jetë d numri më i madh në bashkësinë e faktorëve të përbashkët të a dhe b. Themi se d është **pjesëtuesi**

më i madh i përbashkët i a dhe b, shënuar si $\text{pmmp}(a, b) = d$ dhe nganjëherë $(a, b) = d$. Ngjashëm, mund të definojmë pmmp për më shumë se dy numra.

Ushtrim 1.5. Llogarisni pjesëtuesin më të madh të përbashkët të

- $\text{pmmp}(6, 10)$
- $\text{pmmp}(1, 120)$
- $\text{pmmp}(0, 36)$
- $\text{pmmp}(24, 990, 18)$

Në vijim do të spjegojmë një metodë standarde për gjetjen e pmmp të dy numrave.

Ushtrim 1.6. Gjeni $\text{pmmp}(21, 54)$.

Zgjidhje. Do të zbatojmë të ashtuquajturin **Algoritëm të Euklidit**. Fillimisht, nga pjesëtimi i 54 me 21 kemi

$$54 = 2 \cdot 21 + 12$$

Nga pjesëtimi i 21 me 12 kemi

$$21 = 1 \cdot 12 + 9$$

Nga pjesëtimi i 12 me 9 kemi

$$12 = 1 \cdot 9 + 3$$

Së fundmi kemi

$$9 = 3 \cdot 3 + 0.$$

Sipas algoritmit të Euklidit, mbetja në hapin para se të arrihet mbetja 0 është pmmp e 21 dhe 54. Pra $\text{pmmp}(54, 21) = 3$. □

Ushtrim 1.7.

(a) Gjeni një dyshe numrash të plotë (x, y) ashtu që $760x + 693y = 1$.

(b) Sa dyshe të tilla ekzistojnë?

Zgjidhje.

(a) Që të gjejmë një dyshe (x, y) zbatojmë algoritmin e Euklidit.

$$760 = 1 \cdot 693 + 67$$

$$693 = 10 \cdot 67 + 23$$

$$67 = 2 \cdot 23 + 21$$

$$23 = 1 \cdot 21 + 2$$

$$21 = 10 \cdot 2 + 1$$

Nga ekuacioni i fundit kemi $1 = 21 - 10 \cdot 2$, nga i parafundit kemi $2 = 23 - 1 \cdot 21$. Nëse e vazhdojmë këtë proces dhe i bashkojmë shprehjet kemi

$$1 = 21 - 10 \cdot 2 = 21 - 10 \cdot (23 - 21) = 11 \cdot 21 - 10 \cdot 23.$$

Duke përdorur $21 = 67 - 2 \cdot 23$ kemi

$$1 = 11(67 - 2 \cdot 23) - 10 \cdot 23 = 11 \cdot 67 - 32 \cdot 23.$$

Duke përdorur $23 = 693 - 10 \cdot 67$ kemi

$$1 = 11 \cdot 67 - 32(693 - 10 \cdot 67) = 331 \cdot 67 - 32 \cdot 693.$$

Përfundimisht, përdorim $67 = 760 - 693$ kemi

$$1 = 331(760 - 693) - 32 \cdot 693 = 331 \cdot 760 - 363 \cdot 693.$$

Pra $x = 331$ dhe $y = 363$ është një dyshe për të cilën $760x + 693y = 1$.

(b) Ekzistojnë pafundësisht shumë dyshe të tilla meqë ekzisojnë pafundësisht shumë dyshe (x, y) ashtu që $760x = 693y$.

$\square$

Rezultati në vijim na lejon të karakterizojmë për çfare vlera të a ekzistojnë dyshe të plota (x, y) ashtu që $mx + ny = a$ për m dhe n të fiksuar.

Teoremë 5: Identiteti i Bézout

Për çfarëdo dy numra të plotë m dhe n ekzistojnë numrat e plotë x dhe y ashtu që

$$mx + ny = \text{pmmp}(m, n).$$

Vërtetim. Ekzistenca e një dysheje të plotë (x, y) ashtu që $mx + ny = \text{pmmp}(m, n)$ garantohet nga algoritmi i Euklidit siç kemi parë më herët në rastin $\text{pmmp}(m, n) = 1$. $\square$

Shënim

Vërejmë që nuk mund të fitojmë ndonjë vlerë pozitive më të vogël se $\text{pmmp}(m, n)$ nga $xm + ny$. Kjo meqë $\text{pmmp}(m, n) \mid m$ dhe $\text{pmmp}(m, n) \mid n$ implikon që $\text{pmmp}(m, n) \mid xm + ny$ pra $|\text{pmmp}(m, n)| \leq |xm + ny|$ nëse $xm + ny \neq 0$.

Rrjedhim: Identiteti Gjeneral i Bézout

Për çfarëdo n numra të plotë $a_1, a_2, \ldots, a_n$ ekzistojnë numrat e plotë ashtu që

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = \text{pmmp}(a_1, a_2, \ldots, a_n).$$

Vërtetim. Rrjedhimi mund të vërtetohet me anë të induksionit të fuqishëm. Për ilustrim, tregojmë që nga rasti $n = 2$ mund të fitojmë identitetin e Bézout për $n = 3$.

$$\text{pmmp}(a_1, a_2, a_3) = \text{pmmp}(a_1, \text{pmmp}(a_2, a_3)) = a_1x_1 + c\,\text{pmmp}(a_2, a_3)$$

Përdorim identitetin e Bézout përsëri dhe kemi

$$\text{pmmp}(a_1, a_2, a_3) = x_1a_1 + cx_2a_2 + cx_3a_3.$$

Pra kemi identitetin e Bézout për $n = 3$. Ngjashëm përgjithësojmë për çfarëdo n. Nxënësi inkurajohet ti plotësojë detajet e vërtetimit bazuar në këtë ide. □

Në vijim, do vërtetojmë disa veti të pmmp të cilat do gjejnë zbatim përgjatë këtij materiali.

Ushtrim 1.8. Vërtetoni që nëse $a \mid bc$ dhe $\text{pmmp}(a, b) = 1$, kemi $a \mid c$.

Teoremë 6

(a) Nëse $\text{pmmp}(a, b) = d$ atëherë $a = da'$ dhe $b = db'$ ku a' dhe b' janë numra të plotë dhe $\text{pmmp}(a', b') = 1$.

(b) Nëse $x \mid a$ dhe $x \mid b$, atëherë $x \mid \text{pmmp}(a, b)$.

(c) $\text{pmmp}(ca, cb) = c\,\text{pmmp}(a, b)$.

(d) $\text{pmmp}(a^n, b^n) = \text{pmmp}(a, b)^n$.

(e) $\text{pmmp}(a, b) = \text{pmmp}(a, b \pm n \cdot a)$ për çfarëdo numër të plotë n.[a]

[a] Jashëzakonisht e dobishme!

Vërtetim.

(a) Meqë $d \mid a$ dhe $d \mid b$, kemi $a = da'$ dhe $b = db'$ ku $a', b' \in \mathbb{Z}$. Mjafton të tregojmë që $\text{pmmp}(a', b') = 1$. Supozojmë, për hir të kontradiksionit, që $\text{pmmp}(a', b') = c > 1$. Në këtë rast kemi $a' = ca''$ dhe $b' = cb''$ ku $a'', b'' \in \mathbb{Z}$. Pra duke zëvendësuar për a dhe b kemi se $a = cda''$ dhe $b = cdb''$ pra $cd \mid a$ dhe $cd \mid b$. Meqë $c > 1$, kjo do të thotë se $\gcd(a, b) \geq cd > d$ që bie në kontradiksion me faktin që $\gcd(a, b) = d$. Pra $\text{pmmp}(a', b')$ nuk është më e madhe se 1, rrejdhimisht $\text{pmmp}(a', b') = 1$.

(b) *Ushtrim*

(c) *Ushtrim*

(d) *Ushtrim*

(e) *Ushtrim*

□

Për të ilustruar fuqinë e rezultatit (e) nga teorema paraprake, vërtetojmë teoremën në vijim.

Teoremë 7

Nëse $a, m, n \in \mathbb{N}$, atëherë

$$\text{pmmp}(a^m - 1, a^n - 1) = a^{\text{pmmp}(m,n)} - 1.$$

Vërtetim. Hint: Përdorim vetinë (e) nga teorema paraprake dhe identitetin e Bézout për të zvogëluar fuqinë e a në pmmp. □

Shënim

Një pjesë të madhe të teorisë që kemi zhvilluar mbi pmmp të numrave të plotë mund ta gjeneralizojmë në bashkësi më të sofistikuara se $\mathbb{Z}$. Më poshtë, do të diskutojmë analogun e rezultateve të deritanishme duke zëvendësuar numrat e plotë me polinome me një ndryshore me koeficientë numra racionalë. Megjithatë, kjo nuk është shkalla më e lartë e përgjithësimit të mundshëm. Në fakt, strukturat algjebrike në të cilat vlen algoritmi i Euklidit nga rëndësia fitojnë edhe një emër të veçantë. Ato quhen **Domena Euklidiane**. Megjithatë, fokusi ynë për tani mbetet në rastin $\mathbb{Z}$ dhe $\mathbb{Q}[x]$.

1.2.1 Një Digresion në Polinome

Shënojmë me $\mathbb{Q}[x]$ bashkësinë e polinomeve me një ndryshore me koeficientë numra racionalë. Për të zhvilluar teorinë analoge të pmmp për $\mathbb{Q}[x]$ fillojmë me algoritmin e pjesëtimit.

Teoremë 8: Algoritmi i Pjesëtimit $\mathbb{Q}[x]$

Për çdo dy polinome $a(x)$ dhe $b(x)$ me koeficientë numra racionalë ekziston një dyshe unike e polinomeve në $q(x), r(x) \in \mathbb{Q}[x]$ ashtu që $a(x) = b(x)q(x) + r(x)$ ku $\deg(r) \leq \deg(b)$ ose $r \equiv 0$.

Vërtetim. (se shpejti) □

Ushtrim 1.9. Gjeni $q(x)$ dhe $r(x)$ ashtu që $(x^5 + 3x^4 + 7x^2 + x - 1) = (x^2 - 1)q(x) + r(x)$ ku $q(x), r(x) \in \mathbb{Q}[x]$ dhe $\deg(r) \leq 2$ ose $r \equiv 0$.

Zgjidhje. (se shpejti) □

Definojmë pjesëtuesin më të madh të përbashkët të dy polinoeve $a(x)$ dhe $b(x)$ si polinomin monik me shkallë maksimale që ndanë $a(x)$ dhe $b(x)$. Duke përdorur algoritmin e pjesëtimit për $\mathbb{Q}[x]$ mund të formulojmë algoritmin e Euklidit për $\mathbb{Q}[x]$ dhe një pjesë të madhe të teorisë së zhvilluar për $\mathbb{Z}$. Vërtetimet janë të ngjashme, dhe mbeten si ushtrime për nxënësit.

Teoremë 9

Nëse $a(x) = b(x)q(x) + r(x)$ ashtu që $\deg(r) \leq \deg(b)$, atëherë $\text{pmmp}(a(x), b(x)) = \text{pmmp}(r(x), b(x))$.

Shënim

Duhet të kemi kujdes kur përdorim algoritmin e pjesëtimit ose Euklidit për polinome. Ndonëse për $\mathbb{Q}[x]$ dhe $\mathbb{R}[x]$ këto rezultate vlejnë, për $\mathbb{Z}[x]$ nuk kemi të njejtat. Shembull, $x+1, 2x+1 \in \mathbb{Z}[x]$ por $x+1 = (2x+1)q(x) + r(x)$ për $q(x), r(x) \in \mathbb{Z}[x]$ dhe $\deg(r) \leq 1$ është e pamundur. Pra algoritmi i pjesëtimit nuk vlen për polinome me koeficientë numra të plotë.

1.2.2 Shumëfishi më i Vogël i Përbashkët

Një nocion komplementar i pmmp është ai i shmvp.

Definicion 1.3. Le të jenë a dhe b numra të plotë, jo-zero. Le të jetë m numri më i vogël natyror ashtu që $a \mid m$ dhe $b \mid m$. Themi se m është **shumëfishi më i vogël i përbashkët** i a dhe b, shënuar si $\text{shmvp}(a, b) = m$.

Teoremë 10

Nëse a, b janë numra natyrorë, atëherë $\text{pmmp}(a, b)\,\text{shmvp}(a, b) = ab$.

Vërtetim. Supozojmë që $\text{pmmp}(a, b) = d$. Mund të themi që $a = da'$ dhe $b = db'$ ashtu që $\text{pmmp}(a', b') = 1$. Meqë $ab = d^2a'b'$ mjafton të tregojmë që $\text{shmvp}(a, b) = da'b'$. Le të themi që $m = \text{shmvp}(a, b)$. Duhet të kemi $da' \mid m$ pra $m = da'k_1$. Në anën tjetër, meqë $b \mid m$ kemi $db' \mid da'k_1$ rrjedhimisht $b' \mid a'k_1$. Meqë $\text{pmmp}(a', b') = 1$, kemi $b' \mid k_1$. Pra $k_1 \in \mathbb{N}$ minimal që plotëson $b' \mid k_1$ jep $\text{shmvp}(a, b) = a'b'd$. □

Shënim

Së shpejti do të kemi mundësi të japim një argument shumë më të pastër me ndihmën e numrave të thjeshtë dhe teoremës fundamentale të aritmetikës.

Problemet

Problem 1.10. Tregoni që $\text{pmmp}(n, n+1) = 1$ për çdo $n \in \mathbb{N}$.

Problem 1.11. Duke përdorur algoritmin e Euklidit gjeni

(a) $\text{pmmp}(198, 240)$

(b) $\text{pmmp}(928, 1286)$

(c) pmmp$(12345, 98760)$

(d) pmmp$(2328, 2184, 2604)$

Problem 1.12. Gjeni një dyshe të numrave të plotë (x, y) ashtu që $53x + 77y = 1$.

Problem 1.13. Nëse pmmp$(a, b) = 1$, tregoni që pmmp$(a^2 + b^2 + ab, a + b) = 1$.

Problem 1.14. Gjeni një dyshe të numrave të plotë (x, y) ashtu që $357x + 469y = 7$.

Problem 1.15. Gjeni një dyshe të numrave të plotë (x, y) ashtu që $197x + 131y = 7$.

Problem 1.16. Gjeni një tresha të numrave të plotë (x, y, z) ashtu që $21x + 9y + 35z = 1$.

Problem 1.17. Definojmë $F_n = 2^{2^n} + 1$ për $n \geq 0$. Gjeni pmmp(F_n, F_m).

Problem 1.18. (IMO 1959) Tregoni që për çdo $n \in \mathbb{N}$ thyesa $\dfrac{21n+4}{14n+3}$ është e pathjeshtueshme.

Problem 1.19. Tregoni që për çdo $n \in \mathbb{N}$ kemi

$$\mathrm{pmmp}(n! + 1, (n + 1)! + 1) = 1.$$

Problem 1.20. (HMMT 2002) Sa është vlera e pmmp$(2002 + 2, 2002^2 + 2, 2002^3 + 2, \dots)$.

Problem 1.21. Tregoni se a vlen pmmp(a, b, c) shmvp$(a, b, c) = abc$.

Problem 1.22. (ShBA 1972). Tregoni që

$$\frac{\mathrm{shmvp}(a,b,c)^2}{\mathrm{shmvp}(a,b)\,\mathrm{shmvp}(b,c)\,\mathrm{shmvp}(c,a)} = \frac{\mathrm{pmmp}(a,b,c)^2}{\mathrm{pmmp}(a,b)\,\mathrm{pmmp}(b,c)\,\mathrm{pmmp}(c,a)}.$$

1.3 Numrat e Thjeshtë

Numrat e thjeshtë janë objekti kryesor i studimit në teorinë e numrave. Ata shërbejnë si grimcat elementare nga të cilat të gjithë numrat natyrorë ndërtohen. Njësoj si në kimi ku molekula e ujit ndërtohet nga dy atome hidrogjeni dhe një atom oksigjeni, numri 12 ndërtohet nga dy faktorë të numrit të thjeshte 2 dhe një faktor të numrit të thjeshtë 3. Siç do shohim gjatë këtij materiali, në shumë rast mjafton të kuptojmë ndonjë aspekt të numrave të thjeshtë për të fituar veti të numrave natyrorë. Për shembull, pas një kohe do të vërtetojmë që çdo numër natyror mund të paraqitet si shumë e katër katrorëve të plotë. Hapi i parë i këtij vërtetimi është observimi se mjafton ta vërtetojmë këtë veti për numra të thjeshtë. Fillimisht duhet të definojmë se çka janë numrat e thjeshtë.

Definicion 1.4. Një numër natyror $p \geq 2$ quhet i **thjeshtë** nëse faktorët e vetëm natyrorë të tij janë 1 dhe p.

Ushtrim 1.10. Gjeni 10 numrat e parë të thjeshtë.

Definicion 1.5. Nje numër natyror $n \geq 2$ quhet i **përbërë** nëse nuk është i thjeshtë. Vërejmë që nëse n është i përbërë ekzistojnë dy numra të thjeshte p_1 dhe p_2 (jo detyrimisht të ndryshëm) ashtu që $p_1 p_2 \mid n$. Nga ky observim kemi që nëse n është numër i plotë, n ka një faktor të thjeshtë jo më të madh se $\sqrt{n}$ (plotësoni detajet e implikimit).

Ushtrim 1.11. Nëse p është numër i thjeshtë dhe $p \mid ab$, atëherë $p \mid a$ ose $p \mid b$.

Zgjidhje. Supozojmë që $p \nmid a$. Meqë faktorët e vetëm natyrorë të p janë 1 dhe p, nga supozimi kemi $\text{pmmp}(a, p) = 1$. Nga identiteti i Bézout kemi $ax + py = 1$ për ndonjë dyshe $x, y \in \mathbb{Z}$. Shumëzojmë të dy anët e barazimit me b dhe kemi

$$abx + pyb = b$$

Meqë $p \mid ab$ dhe $p \mid p$, kemi $p \mid abx + pyb$. Pra $p \mid b$. Rrjedhimisht, p duhet të ndajë njërin nga a dhe b. $\square$

Ushtrim 1.12. Nëse $p \mid a^n$, atëherë $p \mid a$.

Zgjidhje. (ushtrim) $\square$

Më poshtë shohim numrat e thjeshte në mesin e 100 numrave të parë natyrorë.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Nese vazhdojme edhe pas 100 shohim se numrat e thjeshtë rrallohen. Por rezultati në vijim tregon që ata asnjëherë nuk mbarojnë. Ky rezultat është vërtetuar nga Euklidi rreth vitit 300 BC. Vërtetimi i kësaj teoreme është një nga aplikimet më të njohura të kontradiksionit.

Teoremë 11: (Euklid, 300 BC)

Ekzistojnë pafundësisht shumë numra të thjeshtë.

Zgjidhje. Supozojmë, për hir të kontradiksionit, që ekziston një bashkësi e fundme $S = \{p_1, p_2, ..., p_n\}$ që përmban të gjithë numrat e thjeshtë. Konsiderojmë numrin $k = p_1 p_2 \ldots p_n + 1$. Meqë $\gcd(k, p_i) = 1$ kemi $p_i \nmid k$ për çdo $i \in \{1, 2, \ldots, n\}$. Pra duke përdorur supozimin kemi që asnjë numër i thjeshtë nuk është faktor i k. Duke qenë se $k > 1$ kemi kontradiksion. Pra ekzistojnë pafundësisht shumë numra të thjeshtë. □

Shënim: 1

Një gabim klasik në argumentin më lartë është konkludimi që k është i thjeshtë meqë nuk ka asnjë faktor në S. Kjo megjithatë nuk vlen detyrimisht. Konsiderojmë $n = 6$ dhe kemi $k = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031$. Por 30031 nuk është i thjeshtë ($30031 = 59 \cdot 509$).

Shënim: 2

Ideja e konstruktimit të k më lart do të paraqitet edhe në të ardhmen siç do të shohim së shpejti.

Meqë bashkësia e numrave të thjeshtë është e pafundme, është e natyrshme të pyesim lidhur me shpërndarjen e numrave të plotë. Një pjesë të madhe të këtyre pyetjeve kërkojnë aparaturë të avancuar nga teoria e numrave analitike të cilën nuk do mund ta zhvillojmë në këtë material. Një pjesë tjetër e pyetjeve qëndrojnë të pazgjidhura për qindra vite. Për shembull, konjektura e të thjeshtëve binjakë është një problem i tillë. Dy numra të thjeshtë quhen **binjakë** nëse kanë distancë 2 mes vete. Konjektura e të thjeshtëve binjakë thotë se ekzistojnë pafundësisht dyshe të tilla. Ky problem mbetet ende i hapur. Megjithatë, ne do të konsiderojmë të kundërtën e këtij problemi. Në vend se të këerkojmë distancë të vogël mes numrave të thjeshtë, ushtrimi në vijim tregon që distanca mes numrave të thjeshtë mund të jetë arbitrarisht e madhe.

Ushtrim 1.13. Vërtetoni që për çdo n mund të gjejmë n numra të njëpasnjëshëm që janë të përbërë.

Zgjidhje. Konstruktimi më i natyrshëm përdor si "bazë" një numër me shumë faktorë. Nëse marrim $(n+1)! + 2$ si numrin e parë, n numrat e njëpasnjëshëm janë:

$$(n+1)! + 2, (n+1)! + 3, \ldots, (n+1)! + (n+1).$$

□

Teorema në vijim formalizon analogjinë mes numrave të thjeshtë dhe llojeve të atomeve. Njësoj sikur teorema mbi pafundësinë e numrave të thjeshtë, teorema në vijim për herë të parë vërtetohet nga Euklidi në librin "Elementet", ndonëse në shkallë më të ulët të gjeneralitetit.

Teoremë 12: Teorema Fundamentale e Aritmetikës

Çdo numër natyror më të madh se 1 mund të shënohet si prodhim i numrave të thjeshtë. Për më tepër, kjo paraqitje është unike.

Pra çdo $n > 1$ mund të shënohet si $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ në mënyrë unike ku p_i janë të thjeshtë dhe $\alpha_k \in \mathbb{N}$.

Vërtetim. (Teknik) Vërtetimi përmban dy pjesë: ekzistencën e një paraqitjeje si produkt i fuqive të numrave të thjeshtë dhe unicitetin e kësaj paraqitje. Fillojmë duke vërtetuar ekzistencën. Përdorim induksionin e fuqishëm në n. *Rasi bazë*: $n = 2$ për të cilin ekziston një paraqitje si produkt i fuqive të thjeshta $(2 = 2)$.
Hipoteza induktive: Supozojmë që ekzistenca vlen për $n = 2, 3, \dots, k$.
Nëse $k+1$ është i thjeshtë, induksioni kompletohet. Supozojmë që $k+1$ nuk është i thjeshtë. Atëherë ekziston një numër i thjeshtë p ashtu që $p \mid k+1$. Pra $k+1 = A \cdot p$. Meqë $A < k+1$, nga hipoteza induktive kemi se ekziston një paraqitje e A si prodhim i fuqive të numrave të thjeshtë. Rrjedhimisht ekziston një paraqitje e $k+1$ si prodhim i fuqive të numrave të thjeshtë. Pra, me anë të induksionit, kemi vërtetuar ekzistencën e një paraqitje si prodhim i fuqive të numrave të thjeshtë për çdo numër natyror.
Në mënyrë që të tregojmë unicitetin e paraqitjes, supozojmë që $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ dhe $n = q_1^{\beta_1} q_2^{\beta_2} \dots q_t^{\beta_t}$. Le të themi se $p_1 < p_2 < ... < p_k$ dhe $q_1 < q_2 < ... < q_t$. Meqë

$$p_1^{\alpha_1} \dots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \dots q_t^{\beta_t}$$

kemi $p_1 \mid q_1^{\beta_1} q_2^{\beta_2} \dots q_t^{\beta_t}$ dhe $q_1 \mid p_1^{\alpha_1} \dots p_k^{\alpha_k}$ duhet të kemi që $p_1 = q_1$. Rrjedhimisht edhe $\alpha_1 = \beta_1$. Ngjashëm edhe për $p_i = q_i$ fitojmë që dy paraqitjet janë identike. □

Shënim

Vetia e faktorizimit unik në elemente të thjeshtë përgjithësohet edhe në unaza (lexo:bashkësi) të tjera përveç $\mathbb{Z}$. Këto quhen **Domena Faktorizimi Unik**. Një rezultat në teorinë e unazave tregon që çdo domenë Euklidiane është domenë faktorizimi unik.

Ushtrim 1.14. Supozojmë që $3n-4$, $4n-5$ dhe $5n-3$ janë numra të thjeshtë. Gjeni n.

Zgjidhje. Vërejmë që shuma e tre numrave është $12n - 12$. Pra shuma është numër çift. Meqë ekziston vetëm një numër i thjeshtë çift, kemi që njëri nga $3n-4$, $4n-5$, ose $5n-3$ është 2.
Nëse $5n - 3 = 2$, kemi $n = 1$ por në këtë rast $4n - 5 = -1$ që nuk është numër i thjeshtë, pra $5n - 3 \neq 2$.
Nëse $4n - 5 = 2$ kemi $n = \dfrac{7}{4}$ por $5n - 3 = \dfrac{35}{4} - 3 \notin \mathbb{N}$. Pra $4n - 5 \neq 2$.
Nëse $3n - 4 = 2$, atëherë $n = 2$. Në këtë rast $4n - 5 = 5$ dhe $5n - 3 = 7$. Pra $n = 2$. □

Ushtrim 1.15. Gjeni numrin më të vogël natyror n ashtu që $\dfrac{n}{2}$ është katror i plotë dhe $\dfrac{n}{3}$ është kub i plotë.

Zgjidhje. Le të themi se $\dfrac{n}{2} = a^2$ dhe $\dfrac{n}{3} = b^3$. Nga këto relacione kemi $n = 2a^2$ dhe $n = 3b^3$.
Nga relacioni i pari kemi $2 \mid n$ dhe nga relacioni i dytë kemi $3 \mid n$.
Pra $n = 6n_1$ dhe kemi $3n_1 = a^2$ dhe $2n_1 = b^3$. Nga këto relacione kemi $3 \mid a^2 \Rightarrow 3 \mid a$ dhe

$2 \mid b^3 \Rightarrow 2 \mid b$.
Pra mund të shënojmë $a = 3a_1$ dhe $b = 2b_1$ dhe kemi $3n_1 = 9a_1^2 \Rightarrow n_1 = 3a_1^2$ dhe $2n_1 = 8b_1^3 \Rightarrow n_1 = 4b_1^3$. Nga këto relacione kemi $3 \mid n_1$ dhe $4 \mid n_1$.
Pra $n_1 = 12n_2$ dhe kemi $12n_2 = 3a_1^2$ dhe $12n_2 = 4b_1^3$. Pra $4n_2 = a_1^2$ dhe $3n_2 = b_1^3$ qe implikon se $4 \mid a_1^2 \Rightarrow 2 \mid a_1$* dhe $3 \mid b_1^3 \Rightarrow 3 \mid b_1$.
Pra $a_1 = 2a_2$ dhe $b_1 = 3b_2$. Rrjedhimisht, $4n_2 = 4a_2^2 \Rightarrow n_2 = a_2^2$ dhe $3n_2 = 27b_2^3 \Rightarrow n_2 = 9b_2^3$.
Pra $n_2 = 9n_3$ dhe kemi $9n_3 = a_2^2$ dhe $9n_3 = 9b_2^3$. Marrim $a_2 = 3a_3$ dhe përfundimisht kemi $n_3 = a_3^2$ dhe $n_3 = b_2^3$.
Për çdo n_3 që është njëkohësisht katror dhe kub i plotë (pra fuqi e gjashtë) fitojmë një n ashtu që $\frac{n}{2}$ është katror i plotë dhe $\frac{n}{3}$ është kub i plotë. Meqë kërkojmë n më të vogël natyror më këtë veti, marrim $n_3 = 1$ dhe fitojmë $n_2 = 9$, $n_1 = 12 \cdot 9 = 108$, dhe $n = 6 \cdot 108 = 648$. □

Teorema fundamentale e aritmetikës na lejon të ri-interpretojmë disa nga konceptet e prezentuara deri tani. Për shembull, nëse kemi $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ dhe $m = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ ku $\beta_i \geq 0$ dhe p_i janë të ndryshme (keni parasysh që për çfarëdo $m, n \in \mathbb{N}$ paraqitja si më lart është e mundur), atëherë

$$\text{pmmp}(m,n) = p_1^{\min\{\alpha_1,\beta_1\}} p_2^{\min\{\alpha_2,\beta_2\}} \dots p_k^{\min\{\alpha_k,\beta_k\}}$$

dhe

$$\text{shmvp}(m,n) = p_1^{\max\{\alpha_1,\beta_1\}} p_2^{\max\{\alpha_2,\beta_2\}} \dots p_k^{\max\{\alpha_k,\beta_k\}}$$

Me këtë paraqitje vërtetimi i teoremës 10 është i drejtpërdrejtë meqë $\alpha_i + \beta_i = \max\{\alpha_i, \beta_i\} + \min\{\alpha_i, \beta_i\}$.

Ushtrim 1.16. (KAMO 2021 7-8) Për një numër natyror $n \neq 1$ shënojmë me a_n faktorin më të madh të numrit n ashtu që $a_n \neq n$ dhe me b_n faktorin më të vogël natyror të numrit n ashtu që $b_n \neq 1$. Gjeni të gjithë numrat natyrorë n për të cilët vlen $\frac{a_n}{b_n} = 17$.

Zgjidhje. □

Ushtrim 1.17. Tregoni që

$$S = 1 + \frac{1}{2} + \dots + \frac{1}{n}$$

nuk është numër i plotë për $n > 1$.

Zgjidhje. Le të jetë $k \in \mathbb{Z}$ ashtu që $2^k \leq n < 2^{k+1}$. Le të jetë m shmvp i numrave $1, 2, 3, \dots, 2^k - 1, 2^k + 1, \dots, n$ (pra n numrave të parë natyrorë përveç 2^k). Shumëzojmë $S = 1 + \frac{1}{2} + \dots + \frac{1}{n}$ me m nga të dyja anët e barazimit dhe kemi

$$mS = m + \frac{m}{2} + \dots + \frac{m}{n}$$

. Në anën e djathtë të ekuacionit secili mbledhor është natyror përveç $\frac{m}{2^k}$ (nga mënyra si kemi definuar k). Pra $mS \notin \mathbb{Z}$, rrjedhimisht $S \notin \mathbb{Z}$. □

*Duhet të kemi kujdes. $4 \mid a_1^2$ nuk implikon $4 \mid a_1$ por vetëm $2 \mid a_1$

Ushtrim 1.18. Le të jetë $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ polinom me koeficientë të plotë ashtu që për katër vlera të ndryshme të plota x_1, x_2, x_3, x_4 kemi $p(x_i) = 5$ për $i \in \{1, 2, 3, 4\}$. Tregoni që nuk ekziston asnjë numër i plotë për të cilin polinomi merr vlerën 12.

Zgjidhje. Meqë $p(x_i) = 5$, kemi

$$p(x) - 5 = (x - x_1)(x - x_2)(x - x_3)(x - x_4)q(x) \tag{1}$$

Supozojmë, për hir të kontradiksionit, që $p(z) = 12$ për $z \in \mathbb{Z}$. Zëvendësojmë $x = z$ në ekuacionin 1 dhe kemi

$$p(z) - 5 = 12 - 5 = (z - x_1)(z - x_2)(z - x_3)(z - x_4)$$

Pra kemi që $12-5 = 7$ është prodhim i katër numrave të ndryshëm* të plotë, por nga teorema fundamentale e aritmetikës kemi se maksimalisht 7 mund të jetë prodhim i tre numrave të ndryshëm të plotë ($7 = (-1) \cdot 1 \cdot (-7)$). Pra kemi kontradiksionin e dëshiruar. □

Ushtrim 1.19. Gjeni të gjithë numrat natyrorë n ashtu që $2^8 + 2^{11} + 2^n$ është katror i plotë.

Zgjidhje. Supozojmë që ekziston një $k \in \mathbb{Z}$ ashtu që $2^8 + 2^{11} + 2^n = k^2$. Meqë $2^8 + 2^{11} = 48^2$ kemi

$$2^n + 48^2 = k^2$$

Rrjedhimisht

$$2^n = (k - 48)(k + 48).$$

Nga teorema fundamentale e aritmetikës kemi që $k-48$ dhe $k+48$ kanë vetëm fuqi të numrit 2 në dekompozimin e tyre në numra të thjeshtë. Pra $k-48 = 2^t$ dhe $k+48 = 2^s$ ku $t+s = n$. Zbresim ekuacionin e parë nga i dyti dhe kemi $k + 48 - (k - 48) = 2^s - 2^t$. Pra

$$96 = 2^s - 2^t$$

Nga ky ekuacion kemi që $2^t \leq 96$. Pra mjafton të shqyrtojmë vlerat e t më të vogla se 7. Zgjidhja e vetme është $t = 5$ dhe $s = 7$ për të cilën kemi $k = 80$ dhe $n = 12$. □

Problemet

Problem 1.23. Verifikoni qe çdo numër n i tillë që $1 < n < 30$ dhe $\text{pmmp}(n, 30) = 1$ është i thjeshtë.
Shënim: 30 është numri më i madh me këtë veti.

Problem 1.24. Themi se dy numra janë **relativisht të thjeshtë** nëse $\text{pmmp}(a, b) = 1$. Nëse a dhe b janë relativisht të thjeshtë dhe ab është katror i plotë, atëherë a dhe b janë katrorë të plotë.

Problem 1.25. Tregoni që në çdo nënbashkësi e $\{1, 2, \ldots, 100\}$ me 51 elemente përmban dy elemente relativisht të thjeshtë njëri-me-tjetrin.

*Pra fakti që x_i janë të ndryshëm është esencial.

Problem 1.26. Tregoni që ekzistonjë pafundësisht numra të thjeshtë të formës $3k+2$.

Problem 1.27. Tregoni që përveç treshes $(0,0,0)$ nuk ekziston asnjë treshe e numrave të plotë (a,b,c) ashtu që
$$a+b\sqrt{2}+c\sqrt{3}=0.$$

Problem 1.28. Tregoni që
$$S=1+\frac{1}{3}+\frac{1}{5}+\cdots+\frac{1}{2n-1}$$
nuk është numër i plotë për $n>1$.

Problem 1.29. Le të jetë $n\geq 2$ dhe $a_1,\ldots,a_n$ numra të plotë jonegativ. Supozojmë që ekziston një numër i thjeshtë p dhe një numër natyror h ashtu që $p^h \mid a_i$ për ndonjë i dhe $p^h \nmid a_j$ për çdo $j\neq i$. Tregoni që
$$S=\frac{1}{a_1}+\cdots+\frac{1}{a_n}$$
nuk është numër i plotë.

Problem 1.30. Tregoni që prodhimi i katër numrave natyrorë të njëpasnjëshëm nuk mund të jetë katror i plotë.

Problem 1.31. Nëse $n>1$, atëherë n^5+n^4+1 nuk është i thjeshtë.

Problem 1.32. Themi se në tokë zbresin disa alienë nga Marsi dhe tregojnë që ata në vend të numrave natyrorë, përdorin bashkësinë $\mathbb{E}$ ku bëjnë pjesë vetëm numrat çiftë[†]. Pra $\mathbb{E}=\{0,2,4,6,\ldots\}$. Le të themi se një numër $a\in\mathbb{E}$ është i $\mathbb{E}$-thjeshtë nëse nuk mund të shënohet si prodhim i dy numrave në $\mathbb{E}$.

(a) Gjeni të gjithë numrat qe janë të $\mathbb{E}$-thjeshte.

(b) Jepni analogun e teoremës fundamentale të aritmetikës për bashkësinë $\mathbb{E}$ dhe numrat e $\mathbb{E}$-thjeshtë. A vlen ekzistenca e një përfaqësimi? A vlen uniciteti?

(c) Gjeni numrin më të vogël në $\mathbb{E}$ që ka 4 përfaqësime të ndryshme si prodhim i numrave të $\mathbb{E}$-thjeshtë.

(d) Cilët numra kanë saktësisht një përfaqësim si prodhim i numrave të $\mathbb{E}$-thjeshtë?

Problem 1.33. Cili është numri më i madh çift i cili nuk mund të paraqitet si shumë e dy numrave të përbërë tekë.

[†]Një shembull i famshëm i këtij lloji është dhënë nga matematikani David Hilbert ku bashkësia përmban numrat e formës $3k+1$. Si ushtrim shtesë mund ti mendoni pjesët (a),(b),(c) dhe (d) edhe për atë bashkësi

Shënim

Problemi më lart i ngjason njërit nga problemet më të famshme dhe vjetra në teorinë e numrave - konjekturës së Goldbahut. Në vitin 1742 matematikani Gjerman Kristian Goldbah hamendësoi se çdo numër çift më i madh se 2 mund të paraqitet si shumë e dy numrave të thjeshtë. Ky problem mbetet ende i pazgjidhur.

1.4 Disa Rregulla të Plotpjesëtueshmërisë

Teoremë 13

Le të jetë $\overline{a_n a_{n-1} ... a_0}$ representimi decimal i numrit a (a_i janë shifra të numrit a).

(a) 2^k ndanë a atëherë dhe vetëm atëher kur 2^k ndanë $\overline{a_{k-1}a_{k-2}...a_0}$

(b) 5^k ndanë a atëherë dhe vetëm atëherë kur 5^k ndanë $\overline{a_{k-1}a_{k-2}...a_0}$

(c) 3 ndanë a atëherë dhe vetëm atëherë kur 3 ndanë $a_n + a_{n-1} + ... + a_0$

(d) 11 ndanë a atëherë dhe vetëm atëherë kur 11 ndanë $a_0 - a_1 + ... + (-1)^n a_n$

Vërtetim.

(a) Vërejmë që $\overline{a_n a_{n-1} \ldots a_0} = 10^k \cdot \overline{a_n a_{n-1} \ldots a_k} + \overline{a_{k-1}a_{k-2} \ldots a_0}$. Meqë $2^k \mid 10^k$ kemi që $2^k \mid \overline{a_n a_{n-1} \ldots a_0} \iff 2^k \mid \overline{a_{k-1}a_{k-2} \ldots a_0}$.

(b) Ngjashëm si në pjesën (a).

(c) Vërejmë që $\overline{a_n a_{n-1} \ldots a_0} = \sum_{i=0}^{n} 10^i a_i$. Meqë 10^i ka mbetje 1 kur pjestohet me 3, kemi që mbetja e $\overline{a_n a_{n-1} \ldots a_0}$ pas pjesëtimit me 3 është mbetja e $a_n + a_{n-1} + \cdots + a_0$ pas pjesëtimit me 3.

(d) Meqë mbetja e 10^i pas pjesëtimit me 11 është ± 1 duke alternuar, si në rastin (c) fitojmë rezultatin e kërkuar.

$\square$

Shënim

Në modulin 2 do të zhvillojmë aparaturë që na lejon të formalizojmë më lehtë vërtetimet e pjesëve (c) dhe (d).

Ushtrim 1.20. Gjeni X dhe Y nëse 8 dhe 9 ndajnë $\overline{X1989Y}$

Zgjidhje. $\square$

Ushtrim 1.21. Gjeni X, Y, dhe Z nëse $3, 5, 8$, dhe 11 ndajnë $\overline{2X4YZ}$

Zgjidhje. □

1.5 Funksionet Multiplikative Tau dhe Sigma

Shënim

Nga tani e tutje, kur themi pjestues nënkuptojmë pjestues natyror. Kur flitet për pjestues potencialisht jo-natyrorë, themi pjestues të plotë.

Teoremë 14

Le të $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ faktorizimi në numra të thjeshtë i numrit n. Shënojmë me $\tau(n)$ numrin e pjestuesve natyrorë n, atëherë $\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$.

Vërtetim. □

Ushtrim 1.22. Nëse $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, sa pjestues të plotë ka n?

Zgjidhje. □

Ushtrim 1.23. Gjeni të gjithë pjestuesit e plotë të numrit 72.

Zgjidhje. □

Ushtrim 1.24. Gjeni prodhimin e pjestuesve natyrorë të 2520.

Zgjidhje. □

Rrjedhim

Për çdo numër natyror n kemi

$$\prod_{d|n} d = n^{\frac{\tau(n)}{2}}.$$

Vërtetim. □

Siç edhe pamë nga teorema 14, numri i pjestuesve të n, varet nga numri i faktorëve të thjeshtë të n dhe jo drejtpërdrejtë nga madhësia e n. Megjithatë, madhësia e n mund të përdoret të na jap një kufi të sipërm të vlerës $\tau(n)$.

Rrjedhim

Për çdo $n \in \mathbb{N}$ kemi
$$\tau(n) \leq 2\sqrt{n}.$$

Vërtetim. □

Teoremë 15

Le të jetë $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ faktorizimi në numra të thjeshtë i numrit n. Shënojmë me $\sigma(n)$ shumën e të gjithë pjestuesve natyrorë të n, atëherë

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \dots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}$$

Vërtetim. □

Ushtrim 1.25. Gjeni shumën e pjestuesve natyrorë të numrit $1,683,000$.

Zgjidhje. □

Ushtrim 1.26. Gjeni shumën e pjestuesve (natyrorë) çiftë të numrit 10000.

Zgjidhje. □

Problemet

Problem 1.34. Llogarisni $\tau(2^n \cdot 3)$, $\sigma(2^n \cdot 3)$.

Problem 1.35. Nëse zgjedhim një pjestues natyror të 10^{70} rastësisht sa është gjasa që ky numër të jetë pjestues i 10^{55}?

Problem 1.36. Gjeni të gjithë n ashtu qe $\sigma(n) = 56$.

Problem 1.37. Gjeni të gjithë n ashtu që $\tau(n)\sigma(n) = 12$.

Problem 1.38. Gjeni të gjithë n ashtu që $\tau(n)\sigma(n) = 20$.

Problem 1.39.

(a) Tregoni që nëse n është numër i thjeshtë, $n \mid \tau(n)\sigma(n) + 2$. Nuk dihet nëse ekziston ndonjë $n > 4$ i përbërë që plotëson këtë veti.

(b) Tregoni që nëse n është numër i thjeshtë, $n \mid \tau(n)\sigma(n) - 2$. Gjeni një numër të përbërë që plotëson këtë veti.

1.6 Një Digresion Lidhur me Konvolucionin e Dirileut

1.7 Probleme Sfiduese për Modulin 1

Problem 1.40. Supozoni që $m \geq n \geq 1$, tregoni që $\frac{\text{pmmp}(m,n)}{m}\binom{m}{n}$ është numër i plotë.

Problem 1.41. Gjeni numrat natyrorë n ashtu që n plotëpjestohet nga çdo numër natyror më i vogël ose baraz me $\sqrt{n}$.

Problem 1.42. (APMO 2004) Gjeni të gjitha bashkësitë (jo të zbrazëta) të fundme S me elemente numra natyrorë ashtu që

$$\frac{i+j}{\gcd(i,j)} \in S$$

për çdo i dhe j (jo meodoemos të ndryshmë) në S.

Problem 1.43. Le të jetë n një numër natyror. Themi se një numër natyror m ka vetinë P nëse $\forall k \in \{1, 2, \ldots, m-1\}$, $\frac{\sigma(m)}{m} > \frac{\sigma(k)}{k}$. Tregoni që ekzistojnë pafundësisht shumë numra me vetinë P.
Shenim: Matematikani Hungarez Paul Erdos në një publikim të vitit 1944 definon numrat me vetinë P si *"Superabundant numbers"*.

Problem 1.44. (IMO 2002/P4)

Problem 1.45. (IMO 1998/P4) Gjeni të gjitha dyshet e numrave natyrorë (a, b) ashtu që

$$ab^2 + b + 7 \mid a^2b + a + b.$$

2 Moduli 2

Deri tani kemi zhvilluar teknika që na lejojnë të flasim për plotpjestueshmëri. Pra krejt në fillim kemi treguar që nëse $a \mid b$ dhe $a \mid c$, atëherë $a \mid b + c$. Do mundohemi që këtë ide ta përgjithësojmë në këtë modul. Pra në vend se të marrim përfundime vetëm për kombinimet lineare të numrave që kanë mbetje 0, do të konsiderojmë edhe kombinimet lineare të numrave që kanë mbetje jo-zero. Në mënyrë që të mbajmë llogari për mbetjet jo-zero, na duhet të zhvillojmë idenë e aritmetikës modulare.

3 Metodat e Vertetimit

3.1 Induksioni Matematik

Teoremë 3.1. Le te jete $P(n)$ nje pohim per variablen n.Atehere nese

- $P(1)$ eshte i sakte dhe
- nese $P(n)$ eshte i sakte atehere edhe $P(n+1)$ eshte i sakte kemi qe $P(n)$ vlen per cdo numer natyror n.

Problem 3.2. Vertetoni qe $1 + 3 + 5 + ... + (2n - 1) = n^2$ per cdo $n \in \mathbb{N}$

Problem 3.3. Vertetoni qe $2^n > n^2$ per cdo $n > 5$

Problem 3.4. Vertetoni qe nje bashkesi me n elemente ka 2^n nenbashkesi.

Teoremë 3.5. Le te jete $P(n)$ nje pohim per variablen n.Atehere nese

- $P(1), P(2), ..., P(k)$ eshte i sakte dhe
- nese $P(n)$ eshte i sakte atehere edhe $P(n+k)$ eshte i sakte kemi qe $P(n)$ vlen per cdo numer natyror n.

Problem 3.6. Vertetoni qe ekuacioni $x^2 + y^2 = z^n$ ka zgjidhje $(x, y, z, n) \in \mathbb{N}^4$ per cdo numer natyror n.

Problem 3.7. Vertetoni qe $9 \mid n^3 + (n+1)^3 + (n+2)^3$ per cdo $n \in \mathbb{N}$

Problem 3.8. Tregoni qe per cdo numer natyror $n > 2$ numrat e formes $2^{2^n} + 1$ mbarojne me shifren 7.

Problem 3.9. (USAMO 2003) Vertetoni qe per cdo numer natyror n ekziston nje numer n-shifror shumefish i 5^n shifrat e te cilit jane te gjitha teke.

Problem 3.10. Vertetoni qe ekzistojne pakufi shume numra natyror qe nuk permbajne shifren 0 dhe qe plotepjesëtohen nga shuma e shifrave te tyre.

4 Sene me i shti

Teoremë 16

Le të jetë n numër natyror dhe $S(n)$ shuma e shifrave të n. Kemi

(a) $9 \mid S(n) - n$

(b) $S(n_1 + n_2) \leq S(n_1) + S(n_2)$

(c) $S(n_1 n_2) \leq \min\{n_1 S(n_2), n_2 S(n_1)\}$

(d) $S(n_1 n_2) \leq S(n_1) S(n_2)$

PSS Engel - 138, 147
BMO 1989 P1 - Kur e bon katrort mod 4.

5 Zgjidhjet e Problemeve

Appendix A - Funksioni i Pjesës së Plotë