19. Uurime jääke!

Täisarvude kohta käivate ülesannete lahendamisel on sageli kasulik uurida avaldiste jääke mingi kindla naturaalarvu (*mooduli*) järgi. Jääkide võttega saab näiteks tõestada, et mõni olukord *ei ole* võimalik. Selleks piisab leida moodul, mille järgi uuritava avaldise jääk ülesande tingimustega vastuolu annab. Sobiva mooduli leidmine nõuab kogemust, tihti omajagu tööd ja vahel natuke õnnegi.

Täisruutude kohta käivate ülesannete lahendamise osutub sageli kasulikuks moodul 4 koos tähelepanekuga, et täisruut saab 4-ga jagamisel anda ainult jäägi 0 või 1. Tõepoolest, paarisarvu $2k$ jaoks saame $(2k)^2 = 4k^2$, mis jagub 4-ga, ning paaritu arvu $2k+1$ jaoks saame $(2k+1)^2 = 4k^2+4k+1$, mis annab 4-ga jagades jäägi 1.

Ülesanne 19.1 (Piirkonnavoor 2009, 10. klass) Matemaatik korrutab enne tööpäeva algust soojenduseks kõik algarvud, mis ei ületa tema vanust päevades, ja liidab saadud korrutisele 1. Kas on võimalik, et ta saab tulemuseks täisarvu ruudu?

Lahendus. Ilmselt on matemaatik vähemalt kaks päeva vana, seega korrutab ta omavahel arvu 2 ja mingi hulga paarituid arve. Saadud korrutis jagub 2-ga, aga mitte 4-ga, niisiis annab see 4-ga jagamisel jäägi 2. Liites veel 1, saab matemaatik lõpuks arvu, mis annab 4-ga jagamisel jäägi 3. Täisruudu jääk jagamisel 4-ga peaks aga olema kas 0 või 1. Seega pole võimalik, et matemaatik saab tulemuseks täiarvu ruudu.

Kuidas aga üldjuhul uurida lõpmatut hulka täisarve? Selgub, et jäägiülesannete puhul piisab, kui vaadata läbi kõiki jäägid, mis antud mooduli n järgi tekida saavad. Neid jääke on aga täpselt n, mida on tunduvalt vähem kui lõpmatu hulk!

Tuletame kõigepealt meelde mõned põhidefinitsioonid.

Definitsioon 19.1 Olgu antud täisarv $n \geqslant 2$ ja suvaline täisarv a. Arvu a *jäägiks* mooduli n järgi (või *modulo* n) nimetame niisugust täisarvu r $(0 \leqslant r \leqslant n-1)$, et

$$a = d \cdot n + r$$

mingi täisarvu d korral.

Lihtne on näha, et kitsendus $0 \leqslant r \leqslant n-1$ määrab jäägi r üheselt.

▪ **Näide 19.1** Täisarvu $a = 2022$ jäägiks jagamisel mooduliga $n = 7$ on $r = 6$, sest kehtib võrdus $2022 = 288 \cdot 7 + 6$.

Paneme tähele, et ka negatiivsest arvust saab mingi positiivse mooduli suhtes jääki leida, kusjuures jääk ise on definitsioonis 19.1 nõutu põhjal mittenegatiivne. Vaatleme näiteks arvu -10 mooduli 7 suhtes. Kuna $-10 = (-2) \cdot 7 + 4$, saame öelda, et -10 annab 7-ga jagades jäägi 4.

Mingi mooduli n suhtes sama jäägi andvad täisarvud asuvad arvteljel nii, et nende vahed on täpselt n. Näiteks arvud, mis annavad mooduli 7 suhtes jäägi 4, on

$$\ldots, -17, -10, -3, 4, 11, 18, \ldots .$$

▪

Definitsioon 19.2 Olgu antud täisarv $n \geqslant 2$. Ütleme, et täisarvud a ja b on *jäägivõrdsed* ehk *kongruentsed* mooduli n järgi, kui a ja b annavad n-iga jagamisel sama jäägi ehk $a - b \vdots n$. Sel juhul kirjutame

$$a \equiv b \bmod n .$$

Definitsiooni 19.2 alusel saame kõik täisarvud antud mooduli n järgi omavahel kongruentsete täisarvude klassideks jagada. Paneme tähele, et vastavaid klasse tekib täpselt n tükki.

▪ **Näide 19.2** Mooduli 4 järgi on neljaks omavahel kongruentsete täisarvude klassiks

$$\{\ldots, -8, -4, 0, 4, 8, \ldots\},$$
$$\{\ldots, -7, -3, 1, 5, 9, \ldots\},$$
$$\{\ldots, -6, -2, 2, 6, 10, \ldots\},$$
$$\{\ldots, -5, -1, 3, 7, 11, \ldots\}.$$

▪

Selline jaotus võimaldabki kõik täisarvud lõpliku töömahuga läbi vaadata. Nimelt osutub, et jääkide kohta käivate väidete uurimiseks piisab, kui vaadata igast klassist läbi üks (näiteks vähim mittenegatiivne) esindaja. Vastava võtte korrektsuse põhjendab järgmine teoreem.

Teoreem 19.1 Olgu antud täisarv $n \geqslant 2$ ning kaks täisarvu a ja b. Olgu r ja s vastavalt nende täisarvude jäägid, mis tekivad jagamisel mooduliga n. Siis kehtivad kongruentsid

$$a + b \equiv r + s \bmod n,$$
$$a - b \equiv r - s \bmod n,$$
$$a \cdot b \equiv r \cdot s \bmod n.$$

Kui m on positiivne täisarv, kehtib lisaks ka kongruents

$$a^m \equiv r^m \bmod n .$$

Tõestus. Definitsiooni 19.1 järgi leiduvad täisarvud d ja e nii, et

$$a = d \cdot n + r \quad \text{ja} \quad b = e \cdot n + s .$$

Siis

$$(a \pm b) - (r \pm s) = d \cdot n \pm e \cdot n = (d \pm e) \cdot n\,.$$

Kuna saadud avaldis jagub n-ga, oleme definitsiooni 19.2 järgi põhjendanud teoreemi kaks esimest kongruentsi. Kolmanda kongruentsi jaoks avaldame

$$a \cdot b - r \cdot s = (d \cdot n + r) \cdot (e \cdot n + s) - r \cdot s = (d \cdot e \cdot n + d \cdot s + r \cdot e) \cdot n\,,$$

mis samuti jagub n-ga. Seega on ka teoreemi kolmas kongruents tõestatud.

Neljanda kongruentsi tõestame induktsiooniga m järgi. Kui $m = 1$, siis $a^1 - r^1 = a - r \vdots n$ ja vajalik kongruents kehtib.

Eeldame nüüd, et mingi täistarvu k korral kehtib $a^k \equiv r^k \bmod n$ ja uurime avaldist $a^{k+1} = a^k \cdot a$. Tänu induktsiooni eeldusele ja ülaltõestatud kolmandale kongruentsile saame

$$a^k \cdot a \equiv r^k \cdot r = r^{k+1}\,,$$

mida oligi induktsiooni sammu lõpetamiseks vaja. □

Nüüd saame sõnastada *jääkide uurimise põhiprintsiibi.*

Olgu antud täisarvuliste muutujatega avaldis, mis kasutab tehetena liitmist, lahutamist, korrutamist ja positiivsete täisarvuliste konstantidega astendamist. Kui on tarvis leida, milliseid jääke saab see avaldis anda jagamisel täisarvuga $n \geqslant 2$, siis piisab, kui leida selle avaldise jäägid n suhtes, andes muutujatele kõikvõimalikud väärtused hulgast $\{0, 1, 2, \ldots, n-1\}$.

Ülesanne 19.2 (Lõppvoor 2005, 9. klass) Olgu a, b ja c suvalised täisarvud. Tõesta, et $a^2 + b^2 + c^2$ jagub 7-ga parajasti siis, kui $a^4 + b^4 + c^4$ jagub 7-ga.

Lahendus. Uurime, milliseid jääke saavad täisarvu ruudud ja neljandad astmed anda jagamisel 7-ga. Ülalsõnastatud printsiibi põhjal piisab, kui uurime, milliseid jääke annavad 7-ga jagamisel arvude $0, 1, 2, 3, 4, 5, 6$ vastavad astmed. Koostame tabeli.

r	r^2	r^4	$r^2 \bmod 7$	$r^4 \bmod 7$
0	0	0	0	0
1	1	1	1	1
2	4	16	4	2
3	9	81	2	4
4	16	256	2	4
5	25	625	4	2
6	36	1296	1	1

Näeme, et tabeli kahes viimases veerus saab kolme jäägi summa jaguda 7-ga ainult siis, kui nad kas kõik on võrdsed 0-ga või kui nad on $1, 2, 4$ mingis järjekorras. Esimene juht vastab olukorrale, kus a, b ja c jaguvad kõik 7-ga ning sel juhul ülesande väide kehtib. Teisel juhul näeme, et r^2 annab 7-ga jagades jäägi 1, 2 või 4 parajasti siis, kui r^4 annab vastavalt jäägi 1, 4 või 2. Niisiis kehtib ülesande väide ka sel juhul.

Ülesande 19.2 lahendamiseks vajaliku tabeli koostamisel saab kasutada mitut nõksu, mis võimaldavad arvudega sadadesse ja tuhandetesse mitte minna. Nii muutub rehkendus ise lihtsamaks, kiiremaks ja vähem veaohtlikuks.

Kõigepealt paneme tähele, et näiteks $6 \equiv -1 \bmod 7$. Seega

$$6^2 \equiv (-1)^2 = 1^2 = 1 \bmod 7.$$

Jah, jäägid tõepoolest toimivad nii! Sama moodi $5 \equiv -2 \bmod 7$ ja $4 \equiv -3 \bmod 7$, järelikult ka

$$5^2 \equiv (-2)^2 = 2^2 = 4 \bmod 7,$$
$$4^2 \equiv (-3)^2 = 3^2 \equiv 2 \bmod 7.$$

Niisiis piisab tabeli $r^2 \bmod 7$ veeru väljaarvutamiseks vaid väärtuste $r = 0, 1, 2, 3$ läbi vaatamisest.

Mida teha veeruga $r^4 \bmod 7$? Selle juures teeb elu lihtsamaks tähelepanek, et

$$r^4 \bmod 7 = (r^2 \bmod 7)^2 \bmod 7.$$

Seega võime veergu $r^4 \bmod 7$ kirjutada lihtsalt eelmise veeru arvude ruudude jäägid jagamisel 7-ga. Kõik vajalikud väärtused oleme seejuures juba eelnevalt välja arvutanud. Kokkuvõttes polnud arvutustes vaja arvudega kordagi isegi kümnetesse minna!

Ülesanded

Ülesanne 19.3 (Piirkonnavoor 2002, 9. klass, b)-osa) Kas leidub naturaalarve, mille ruut avaldub nelja järjestikuse naturaalarvu summana?

Ülesanne 19.4 (Sügisene lahtine võistlus 2019, noorem rühm) Leia kõik algarvud p, mille korral ka $\frac{p-1}{2}$ ja $\frac{p+1}{4}$ on algarvud.

Ülesanne 19.5 (Talvine lahtine võistlus 2011, noorem rühm) Tõesta, et võrrandil

$$2x^3 - y^2 = 3$$

ei ole täisarvulisi lahendeid.

Ülesanne 19.6 (Piirkonnavoor 2010, 9. klass) Leia kõik jäägid, mille saab anda 4-ga mittejaguva paarisarvu ruut jagamisel 32-ga.

Ülesanne 19.7 (Lõppvoor 2012, 9. klass) Täisarvude a, b, c kohta on teada, et $a+b+c$ jagub 6-ga ja $a^2+b^2+c^2$ jagub 36-ga. Kas võib kindlalt väita, et arv $a^3+b^3+c^3$ jagub

a) 8-ga?

b) 27-ga?

Ülesanne 19.8 (Sügisene lahtine võistlus 2009, noorem rühm) Leia kõik positiivsed täisarvud n , mille korral $1+2^2+3^3+4^n$ on mingi täisarvu ruut.

Ülesanne 19.9 (Lõppvoor 2021, 9. klass) Mängijad A, B ja C mängivad järgmist mängu. Alguses on tahvlil arv 1. Oma käigul asendab mängija parajasti tahvlil oleva arvu n omal valikul kas arvuga $n+1$, arvuga $7n+7$ või arvuga $4n^3+3n+4$, kuid kirjutatav arv ei tohi olla suurem kui 10^9. Käiakse kordamööda: alustab A, seejärel käib B, siis C, tema järel jälle A jne kuni käigupuuduse tekkimiseni. Võidab mängija, kes teeb viimase käigu. Kas ühel mängijaist on võimalik võita teiste suvalise vastumängu korral ja kui jah, siis kellel?

Ülesanne 19.10 (Lõppvoor 2021, 10. klass) Leia kõik positiivsed täisarvud k, mille korral leidub täisnurkne kolmnurk, mille kaatetite pikkused on täisarvulised ning mille hüpotenuusi pikkus on $\sqrt{88\ldots822\ldots2}$, kus juure all olevas arvus on täpselt k kaheksat ja täpselt k kahte.

Ülesanne 19.11 (Piirkonnavoor 2018, 11. klass) Keraamik valmistab risttahukakujulise tellise, mille servapikkused on täisarvud a, b ja c, kusjuures $\text{SÜT}(a,b) = \text{SÜT}(b,c) = \text{SÜT}(c,a) = 1$. Kas selle tellise vastastippe ühendava diagonaali pikkus saab olla täisarv?

Ülesanne 19.12 (Lõppvoor 1993, 11. klass) Tõesta, et ühegi naturaalarvu $n \geqslant 1$ korral ei saa arvu

$$1+2+\ldots+n$$

viimaseks numbriks olla $2, 4, 7$ ega 9.

Ülesanne 19.13 (Piirkonnavoor 2003, 12. klass) Milliste täisarvude n korral jagub arv n^4+n^2-2 arvuga 72?

Ülesanne 19.14 (Piirkonnavoor 1998, 12. klass) Leia kõik võimalikud jäägid, mis võivad tekkida algarvu $p>3$ ruudu p^2 jagamisel arvuga 12.

Ülesanne 19.15 (Piirkonnavoor 2022, 12. klass) Arvujadas (a_n) kehtivad võrdused $a_1 = 4, a_2 = -7$ ning $a_n = a_{n-1}a_{n-2} - 1$ iga $n > 2$ korral. Kas leidub selline algarv, millega jada (a_n) ükski liige ei jagu?

Ülesanne 19.16 (Sügisene lahtine võistlus 2009, vanem rühm) Kas leidub selline algarv p, et p^3+2008 ja p^3+2010 on samuti algarvud?

Ülesanne 19.17 (Sügisene lahtine võistlus 2012, vanem rühm) Leia kõik jäägid, mille saab 6-ga jagamisel anda täisarv n, mis rahuldab võrdust $n^3 = m^2+m+1$ mingi täisarvu m korral.

Ülesanne 19.18 (Piirkonnavoor 2008, 12. klass) Olgu a ja b täisarvud. Tõesta, et kui $ab+1$ jagub 8-ga, siis ka $a+b$ jagub 8-ga.

Ülesanne 19.19 (Lõppvoor 1995, 10. klass) Tõesta, et kui m ja n on naturaalarvud ning arv $mn+1$ jagu arvuga 24, siis arv $m+n$ jagub samuti arvuga 24.

Ülesanne 19.20 (Lõppvoor 2000, 11. klass) Leia kõik algarvud, mille kuues aste ei anna 504-ga jagades jäägiks 1.

Ülesanne 19.21 (Lõppvoor 2007, 11. klass) Leia kõik positiivsete täisarvude paarid (m,n), mille korral

$$m^n - n^m = 3\,.$$

Ülesanne 19.22 (Lõppvoor 2005, 11. klass) Kas leidub selline täisarv $n > 1$, et arv

$$2^{2^n-1} - 7$$

ei ole ühegi täisarvu ruut?

Ülesanne 19.23 (Lõppvoor 2009, 12. klass) Olgu n mittenegatiivne täisarv, mille korral

$$3^n + 3^{n+1} + \ldots + 3^{2n}$$

on täisarvu ruut. Tõesta, et n jagub 4-ga.

Ülesanne 19.24 (Piirkonnavoor 2022, 11. klass) Kas leiduvad täisarvud x ja y, mille korral

a) $x^2 - xy + y^2 = 2021$?

b) $x^2 - xy + y^2 = 2022$?

Ülesanne 19.25 (Talvine lahtine võistlus 2018, vanem rühm) Positiivsete täisarvude a ja b korral on murru

$$\frac{5a^4 + a^2}{b^4 + 3b^2 + 4}$$

väärtus täisarv. Tõesta, et a on kordarv.

Ülesanne 19.26 (Sügisene lahtine võistlus 1999, vanem rühm) Leia kõik jäägid, mis saavad tekkida 120-ga ühistegurita arvu ruudu jagamisel 120-ga.

Ülesanne 19.27 (Sügisene lahtine võistlus 2006, vanem rühm) Olgu b positiivne paarisarv, mille korral leidub naturaalarv $n > 1$ nii, et arv $\dfrac{b^n - 1}{b - 1}$ on täisarvu ruut. Tõesta, et b jagub 8-ga.

Lahendused

19.3 Vastus: ei.

Nelja järjestikuse naturaalarvu $n, n+1, n+2$ ja $n+3$ summa on $4n+6$, mis annab 4-ga jagades jäägi 2. Naturaalarvude ruudud aga saavad 4-ga jagades anda ainult jääke 0 ja 1.

19.4 Vastus: 7 ja 11.

Lahenduse võtmeks on leida moodul, mille järgi õnnestub näidata, et $\dfrac{p-1}{2}$ ja $\dfrac{p+1}{4}$ on enamasti kordarvud. Moodul 2 ei anna midagi mõistlikku, aga 3 sobib.

Kõigepealt näeme, et kui $p = 3$, siis $\dfrac{p-1}{2} = \dfrac{p+1}{4} = 1$ pole algarv. Muude algarvude korral peab kehtima kas $p \equiv 1 \bmod 3$ või $p \equiv 2 \bmod 3$.

Kui $p \equiv 1 \bmod 3$, siis eeldusel, et $\frac{p-1}{2}$ on täisarv, peab kehtima $\frac{p-1}{2} \vdots 3$. Kuna tegemist peab olema algarvuga, saame, et sel juhul $\frac{p-1}{2} = 3$, kust omakorda $p = 7$. Teisest küljest on siis ka $\frac{p+1}{4} = 2$ algarv.

Kui $p \equiv 2 \bmod 3$, siis eeldusel, et $\frac{p+1}{4}$ on täisarv, peab kehtima $\frac{p+1}{4} \vdots 3$. Kuna tegemist peab olema algarvuga, saame, et sel juhul $\frac{p+1}{4} = 3$, kust omakorda $p = 11$. Teisest küljest on siis ka $\frac{p-1}{2} = 5$ algarv.

19.5 Kuna $2x^3$ on paaris ja 3 paaritu, peab y^2 olema paaritu, seega peab ta olema paaritu arvu ruut ja esituma kujul $y^2 = (2n+1)^2 = 4n^2+4n+1$ mingi täisarvu n jaoks. Järelikult

$$2x^3 = 4n^2+4n+4 = 4(n^2+n+1).$$

Niisiis $2x^3 \vdots 4$, mis tähendab, et x peab olema paarisarv ja muuhulgas $2x^3 \vdots 16$. Nüüd aga saame vastuolu, sest $n^2+n+1 = n(n+1)+1$ on kindlasti paaritu, mistõttu $4(n^2+n+1)$ ei saa jaguda 16-ga. Seega ei saa algsel võrrrandil olla lahendeid täisarvudes.

19.6 Vastus: ainus võimalik jääk on 4.

4-ga mittejaguva paarisarvu üldkuju on $4k+2$ (kus $k \in \mathbb{Z}$). Seda ruutu tõstes saame

$$(4k+2)^2 = 16k^2+16k+4 = 16k(k+1)+4.$$

Kuna üks arvudest k ja $k+1$ on kindlasti paarisarv, peab arv $16k(k+1)$ jaguma 32-ga ning $(4k+2)^2$ võib järelikult 32-ja jagades anda ainult jäägi 4.

Seda ülesannet saab lahendada ka jääkide uurimise põhiprintsiibi abil, aga tööd on natuke rohkem. Kõigepealt paneme tähele, et 4-ga mittejaguv paarisarv saab 32-ga jagades anda ainult jääke $2, 6, 10, 14, 18, 22, 26$ ja 30. Vaatame läbi nende ruutude jäägid, mis tekivad jagamisel 32-ga:

$$\begin{aligned}
2^2 &= 4 \equiv 4 \bmod 32,\\
6^2 &= 36 \equiv 4 \bmod 32,\\
10^2 &= 100 \equiv 4 \bmod 32,\\
14^2 &= 196 \equiv 4 \bmod 32,\\
18^2 &= 324 \equiv 4 \bmod 32,\\
22^2 &= 484 \equiv 4 \bmod 32,\\
26^2 &= 676 \equiv 4 \bmod 32,\\
30^2 &= 900 \equiv 4 \bmod 32.
\end{aligned}$$

Niisiis näeme jälle, et tekkida saab ainult jääk 4.

19.7 Vastus: a) jah, b) ei.

a) Näitame, et kui $a+b+c \vdots 2$ ja $a^2+b^2+c^2 \vdots 4$, siis peavad a, b ja c olema paarisarvud. Sellest väitest järeldub kohe, et $a^3+b^3+c^3 \vdots 8$.

Kui $a+b+c \vdots 2$, aga nad kõik ei ole paarisarvud, peab a, b ja c seas leiduma täpselt kaks paaritut arvu. Paarisarvu ruut annab 4-ga jagades jäägi 0, paaritu

arvu ruut aga jäägi 1. Niisiis peab $a^2+b^2+c^2$ andma 4-ga jagades jäägi 2; saime vastuolu eeldusega $a^2+b^2+c^2 \vdots 4$.

b) Sobiva konstruktsiooni annab näiteks valik $a=2$, $b=2$ ja $c=8$. Siis $a+b+c = 12 \vdots 6$ ja $a^2+b^2+c^2 = 72 \vdots 36$, aga $a^3+b^3+c^3 = 528 \not\vdots 27$.

19.8 Vastus: $n=1$ on ainus võimalus.

Kui $n=1$ ja $n=2$, siis on ülesande avaldise väärtuseks vastavalt 36 ja 48; neist esimene on täisruut ja teine ei ole. Kui $n>2$, saame ülesande avaldist teisendada järgmiselt:

$$1+2^2+3^3+4^n = 32+4^n = 16\cdot(2+4^{n-2}).$$

Et selle avaldise väärtus saaks olla täisruut, peaks täisruut olema ka $2+4^{n-2}$. Samas kui $n>2$, saame $2+4^{n-2} \equiv 2 \bmod 4$. Täisruudud aga saavad 4-ga jagades anda ainult jäägi 0 või 1. Niisiis rohkem võimalusi ei ole.

19.9 Vastus: võitev strateegia on mängijal C.

Lahenduse võtmeks on vaadelda tahvlil oleva arvu jääki jagamisel 3-ga. Paneme tähele, et iga lubatud käik muudab seda jääki tsükliliselt 1 võrra suuremaks (st jäägist 1 saab jääk 2, jäägist 2 jääk 0 ja jäägist 0 jääk 1).

See väide on ilmne käigu $n \to n+1$ jaoks. Käigu $n \to 7n+7$ puhul on asi samuti lihtne, sest $7 \equiv 1 \bmod 3$ ja järelikult ka

$$7n+7 \equiv n+1 \bmod 3.$$

Käigu $n \to 4n^3+3n+4$ korral paneme kõigepealt tähele, et $n^3 \equiv n \bmod 3$ iga täisarvu n jaoks. Selles võime veenduda jääkide uurimise põhiprintsiibi abil, vaadates läbi jäägid 0, 1 ja 2:

$$0^3 = 0 \equiv 0 \bmod 3,$$
$$1^3 = 1 \equiv 1 \bmod 3,$$
$$2^3 = 8 \equiv 2 \bmod 3.$$

Loomulikult kehtivad ka kongruentsid $4 \equiv 1 \bmod 3$ ja $3 \equiv 0 \bmod 3$, järelikult

$$4n^3+3n+4 \equiv 1n+0n+1 = n+1 \bmod 3.$$

Niisiis on pärast A käiku tahvlil alati arv, mis annab 3-ga jagades jäägi 2, pärast B käiku arv, mis annab 3-ga jagades jäägi 0, ning pärast C käiku arv, mis annab 3-ga jagades jäägi 1.

Kuna tahvlil oleva arvu suurendamine 1 võrra on alati lubatud, lõppebki mäng parajasti siis, kui tahvlile ilmub 10^9. Kuna $10^9 \equiv 1^9 = 1 \bmod 3$, peab viimase käigu tegija olema mängija C.

19.10 Vastus: $k=1$ on ainus võimalus.

Pythagorase teoreemi põhjal otsime võrrandi

$$a^2+b^2 = 88\ldots822\ldots2$$

täisarvulisi lahendeid.

Kui $k=1$, siis sobivad $a=1$ ja $b=9$, sest $a^2+b^2=82$.

Kui $k \geqslant 2$, siis otsime moodulit, mille järgi ülaltoodud võrrand kehtida ei saa.

Ruutude puhul töötab tihti moodul 4, aga praegu pole temast kasu, sest kehtib seos $88\ldots822\ldots2 \equiv 2 \bmod 4$ ning kui a ja b on paaritud, annab nende ruutude summa samuti 4-ga jagades jäägi 2. Sama moodi ei anna tulemust ka moodulid $2,3,5,6$ ja 7.

Aga mooduli 8 järgi näeme, et $88\ldots822\ldots2 \equiv 6 \bmod 8$, sest nii $822 \equiv 6 \bmod 8$ kui ka $222 \equiv 6 \bmod 8$. Teisest küljest saavad täisarvude ruudud anda 8-ga jagades ainult jäägi $0,1$ või 4. Selles väites saame veenduda näiteks jääkide uurimise põhiprintsiibi järgi, kontrollides arvude $0,1,\ldots,7$ ruute:

$$\begin{aligned}
0^2 &= 0 \equiv 0 \bmod 8,\\
1^2 &= 1 \equiv 1 \bmod 8,\\
2^2 &= 4 \equiv 4 \bmod 8,\\
3^2 &= 9 \equiv 1 \bmod 8,\\
4^2 &= 16 \equiv 0 \bmod 8,\\
5^2 &= 25 \equiv 1 \bmod 8,\\
6^2 &= 36 \equiv 4 \bmod 8,\\
7^2 &= 49 \equiv 1 \bmod 8.
\end{aligned}$$

Järelikult ei saa kahe täisarvu ruudu summa anda 8-ga jagades jääki 6, sest võimalikud tekkivad jäägid on ainult $0,1,2,4$ ja 5.

19.11 Vastus: ei.

Tellise diagonaali pikkus d avaldub servapikkuste kaudu kujul $d^2 = a^2 + b^2 + c^2$. Kuna servapikkused a, b ja c on paarikaupa ühistegurita, saab ülimalt üks neist olla paaris. Niisiis annavad kaks või kolm arvudest a^2, b^2 ja c^2 jagamisel 4-ga jäägi 1 ja üks või mitte ükski jäägi 0. Järelikult on summa $a^2 + b^2 + c^2$ jääk jagamisel 4-ga kas 2 või 3. Täisruudu d^2 jääk jagamisel 4 peaks aga olema kas 0 või 1.

19.12 Aritmeetilise jada summa valemist teame, et

$$1 + 2 + \ldots + n = \frac{n(n+1)}{2}.$$

Uurime, milliseid väärtusi võib võtta avaldise $n(n+1)$ viimane number, st jääki jagamisel 10-ga. Jääkide uurimise põhiprintsiibi järgi teame, et selleks piisab uurida väärtusi $n = 0,1,\ldots,9$. Näeme, et

$$\begin{aligned}
&0 \cdot 1 = 0, 1 \cdot 2 = 2, 2 \cdot 3 = 6, 3 \cdot 4 = 12, 4 \cdot 5 = 20,\\
&5 \cdot 6 = 30, 6 \cdot 7 = 42, 7 \cdot 8 = 56, 8 \cdot 9 = 72, 9 \cdot 10 = 90.
\end{aligned}$$

Niisiis saavad avaldise $n(n+1)$ viimaste numbritena esineda ainult $0,2$ ja 6. Järelikult saavad avaldise $\dfrac{n(n+1)}{2}$ viimased numbrid olla ainult $0,5,1,6,3$ ja 8.

19.13 Vastus: $n^4 + n^2 - 2 \vdots 72$ täpselt nende täisarvude n korral, mis ei jagu ei 2-ga ega 3-ga.

Täisarv jagub 72-ga parajasti siis, kui ta jagub 8-ga ja 9-ga. Uurime avaldise $n^4 + n^2 - 2$ jääki jagamisel 8-ga ja 9-ga, kui n võtab kõik väärtused vastavalt 0-st 7-ni ja 0-st 8-ni. Seejuures osutuvad väga kasulikuks võtted, millega tutvusime

ülesande 19.2 lahenduse järel. Leiame vaheväärtustena n^2 ja n^4 jäägid jagamisel 8 ja 9-ga. Lisaks peame meeles, et $7 \equiv -1 \bmod 8, 6 \equiv -2 \bmod 8, \ldots, 8 \equiv -1 \bmod 9$ jne, mis võimaldab piirduda ainult poole n^2 veeru väljaarvutamisega.

n	$n^2 \bmod 8$	$n^4 \bmod 8$	$(n^4+n^2-2) \bmod 8$
0	0	0	6
1	1	1	0
2	4	0	2
3	1	1	0
4	0	0	6
5	1	1	0
6	4	0	2
7	1	1	0

n	$n^2 \bmod 9$	$n^4 \bmod 9$	$(n^4+n^2-2) \bmod 9$
0	0	0	7
1	1	1	0
2	4	7	0
3	0	0	7
4	7	4	0
5	7	4	0
6	0	0	7
7	4	7	0
8	1	1	0

Näeme, et $n^4+n^2-2 \equiv 0 \bmod 8$ parajasti siis, kui n ei jagu 2-ga, ja $n^4+n^2-2 \equiv 0 \bmod 9$ parajasti siis, kui n ei jagu 3-ga. Seega $n^4+n^2-2 \equiv 0 \bmod 72$ parajasti siis, kui n ei jagu ei 2-ga ega 3-ga.

Selle ülesande teise võimaliku lahenduse annab ülesanne 22.7.

19.14 Vastus: ainus võimalik jääk on 1.

Kõikvõimalikud jäägid, mis saavad tekkida positiivse täisarvu p jagamisel 12-ga, saame kätte, kui vaatame p kohal läbi jäägid $0, 1, 2, \ldots, 11$. Kuna p peab lisaks olema 3-st suurem algarv, siis teame, et väärtusi $0, 2, 3, 4, 6, 8, 9, 10$ pole mõtet vaadelda. Niisiis piisab, kui uurime väärtusi $p = 1, 5, 7, 11$. Nende puhul saame

$$\begin{aligned} 1^2 = 1 &\equiv 1 \bmod 12, \\ 5^2 = 25 &\equiv 1 \bmod 12, \\ 7^2 = 49 &\equiv 1 \bmod 12, \\ 11^2 = 121 &\equiv 1 \bmod 12. \end{aligned}$$

Niisiis saab tekkida ainult jääk 1.

19.15 Vastus: jah, sobib näiteks 11.

Leiame vaadeldava jada mõned esimesed liikmed: $a_1 = 4$, $a_2 = -7$, $a_3 = 4 \cdot (-7) - 1 = -29$, $a_4 = (-7) \cdot (-29) - 1 = 202$. Lihtne on näha, et $a_1 \equiv a_2 \equiv 4 \bmod 11$ ning samuti $a_3 \equiv 4 \bmod 11$ ja $a_4 \equiv 4 \bmod 11$.

Tekib hüpotees, et jada kõik liikmed annavad 11-ga jagades jäägi 4. Hüpoteesi tõestamiseks saame kasutada matemaatilist induktsiooni. Induktsiooni baas on

jada esimeste liikmete jaoks juba kontrollitud. Sammu tegemiseks paneme tähele, et kui $a_{n-1} \equiv a_{n-2} \equiv 4 \bmod 11$, siis

$$a_n = a_{n-1}a_{n-2} - 1 \equiv 4 \cdot 4 - 1 = 15 \equiv 4 \bmod 11\,.$$

Niisiis ei jagu jada (a_n) ükski liige 11-ga.

19.16 Vastus: ei.

Niisuguste üleaannete puhul on sageli kasulik muutujate väikeseid väärtusi läbi proovida. Selle peale juhtub tüüpiliselt üks kahest – me kas jõuame väärtuseni, mis rahuldab ülesande tingimusi, või leiame seaduspära, mis aitab põhjendada miks niisugust väärtust ei leidu.

Proovime väikeseid algarve läbi ning leiame p^3+2008 ja p^3+2010 tegurdused.[1]

p	p^3+2008	p^3+2010
2	$2^5 \cdot 3^2 \cdot 7$	$2 \cdot 1009$
3	$5 \cdot 11 \cdot 37$	$3 \cdot 7 \cdot 97$
5	$3^3 \cdot 79$	$5 \cdot 7 \cdot 61$
7	2351	$13 \cdot 181$
11	$3^2 \cdot 7 \cdot 53$	$13 \cdot 257$
13	$5 \cdot 29^2$	$7 \cdot 601$

Tabelist hakkab silma, et igas reas peale 7 jagub üks arvudest p^3+2008 ja p^3+2010 7-ga. Kas me suudame selle reegli üldjuhul tõestada?

Uurime avaldiste a^3+2008 ja a^3+2010 jääki jagamisel 7-ga. Kõigepealt paneme tähele, et $2008 \equiv 6 \bmod 7$ ja $2010 \equiv 1 \bmod 7$, seega piisab vaadelda avaldisi a^3+6 ja a^3+1.

Kuna algarv 7 on tabelis juba läbi vaadatud, piisab, kui uurime mittenulljääke, mis 7-ga jagamisel tekkida võivad, st väärtusi $a = 1,2,3,4,5,6$. Koostame vastava tabeli.

a	a^3+6	a^3+1
1	**7**	2
2	**14**	9
3	33	**28**
4	**70**	65
5	131	**126**
6	222	**217**

Näeme, et igal juhul jagub üks väärtus tabeli reas 7-ga, seega nõutud omadusega algarve ei leidu.

19.17 Vastus: 1 on ainus selline jääk.

Uurime kõigepealt, milliseid jääke saab anda n^3 jagamisel 6-ga. Jääkide uuri-

[1] Praktikas pole kõiki arve lõpuni tegurdada vaja. Piisab, kui leiame proovimise teel mõned väiksemad algtegurid.

mise põhiprintsiibi alusel piisab, kui vaatleme arvude $0,1,\ldots,5$ kuupide jääke:

$$\begin{aligned}
0^3 &= 0 \equiv 0 \bmod 6,\\
1^3 &= 1 \equiv 1 \bmod 6,\\
2^3 &= 8 \equiv 2 \bmod 6,\\
3^3 &= 27 \equiv 3 \bmod 6,\\
4^3 &= 64 \equiv 4 \bmod 6,\\
5^3 &= 125 \equiv 5 \bmod 6.
\end{aligned}$$

Siit mingeid kitsendusi ei tule – kõik võimalikud jäägid tõepoolest esinevad.

Proovime õnne avaldisega m^2+m+1, kuhu asendame sama moodi väärtused $0,1,\ldots,5$:

$$\begin{aligned}
0^2+0+1 &= 1 \equiv 1 \bmod 6,\\
1^2+1+1 &= 3 \equiv 3 \bmod 6,\\
2^2+2+1 &= 7 \equiv 1 \bmod 6,\\
3^2+3+1 &= 13 \equiv 1 \bmod 6,\\
4^2+4+1 &= 21 \equiv 3 \bmod 6,\\
5^2+5+1 &= 31 \equiv 1 \bmod 6.
\end{aligned}$$

Nüüd läks paremini – näeme, et esineda võivad ainult jäägid 1 ja 3. Ülaltehtud arvutuste põhjal n^3 jaoks tähendab see, et $n \equiv 1 \bmod 6$ või $n \equiv 3 \bmod 6$.

Konstruktsioon $n \equiv 1 \bmod 6$ jaoks on lihtne: kui $n=1$, siis sobivad nii $m=0$ kui $m=-1$.

Näitame et variant $n \equiv 3 \bmod 6$ pole võimalik. Paneme tähele, et kui $n \equiv 3 \bmod 6$, siis $n^3 \vdots 9$. Uurime avaldise m^2+m+1 võimalikke jääke jagamisel 9-ga:

$$\begin{aligned}
0^2+0+1 &= 1 \equiv 1 \bmod 9,\\
1^2+1+1 &= 3 \equiv 3 \bmod 9,\\
2^2+2+1 &= 7 \equiv 7 \bmod 9,\\
3^2+3+1 &= 13 \equiv 4 \bmod 9,\\
4^2+4+1 &= 21 \equiv 3 \bmod 9,\\
5^2+5+1 &= 31 \equiv 4 \bmod 9.\\
6^2+6+1 &= 43 \equiv 7 \bmod 9,\\
7^2+7+1 &= 57 \equiv 3 \bmod 9,\\
8^2+8+1 &= 73 \equiv 1 \bmod 9.
\end{aligned}$$

Näeme, et igal juhul $m^2+m+1 \not\vdots 9$.

19.18 Kui $ab+1$ jagub 8-ga, peavad a ja b olema paaritud arvud. Niisiis piisab jääkide uurimise põhiprintsiibi järgi, kui vaatame a ja b kohal läbi paaritute arvude jäägid jagamisel 8-ga, st $1,3,5$ ja 7. Koostame tabeli, kuhu kirjutame $ab+1$ jäägid jagamisel 8-ga, mis kõikidel võimalikel juhtudel tekivad.

	1	3	5	7
1	2	4	6	0
3	4	2	0	6
5	6	0	2	4
7	0	6	4	2

Tabelist näeme, et jäägi 0 saame ainult neil juhtudel, kui $a+b \equiv 0 \bmod 8$ ehk $a+b \vdots 8$.

19.19 Mooduli 8 järgi on tegemist täpselt ülesande 19.18 väitega. Niisiis jääb üle kontrollida sama väite paikapidavust mooduli 3 järgi.

Jääkide uurimise põhiprintsiibi järgi piisab kui uurime, millise jäägi annab 3-ga jagades suurus $mn+1$, kui $m, n \in \{0,1,2\}$. Koostame vastava tabeli.

	0	1	2
0	1	1	1
1	1	2	0
2	1	0	2

Näeme, et $mn+1 \vdots 3$ parajasti siis, kui üks arvudest m ja n annab 3-ga jagades jäägi 1 ja teine jäägi 2. Sel juhul aga ka $m+n \vdots 3$.

19.20 Vastus: 2, 3 ja 7.

Tegurdades leiame, et $504 = 7 \cdot 8 \cdot 9$, järelikult ei saa $2^6, 3^6$ ja 7^6 anda 504-ga jagades jääki 1.

Näitame, et kõigi teiste algarvude p korral $p^6 \equiv 1 \bmod 504$ ehk $p^6 - 1 \vdots 504$. Selleks tõestame, et algarvude $p \notin \{2,3,7\}$ puhul $p^6 - 1 \vdots 7$, $p^6 - 1 \vdots 8$ ja $p^6 - 1 \vdots 9$ ehk $p^6 \equiv 1 \bmod 7$, $p^6 \equiv 1 \bmod 8$ ja $p^6 \equiv 1 \bmod 9$.

Jääkide uurimise põhiprintsiibi alusel piisab, kui uurime ainult jääke, mida algarv p vastava mooduli suhtes anda võib.

Mooduli 7 suhtes tuleb läbi vaadata jäägid $1, 2, \ldots, 6$:

$$\begin{aligned} 1^6 = 1 &\equiv 1 \bmod 7, \\ 2^6 = 64 &\equiv 1 \bmod 7, \\ 3^6 = 729 &\equiv 1 \bmod 7, \\ 4^6 \equiv (-3)^6 = 3^6 &\equiv 1 \bmod 7, \\ 5^6 \equiv (-2)^6 = 2^6 &\equiv 1 \bmod 7, \\ 6^6 \equiv (-1)^6 = 1^6 &\equiv 1 \bmod 7. \end{aligned}$$

Mooduli 8 suhtes tuleb läbi vaadata jäägid $1, 3, 5, 7$:

$$\begin{aligned} 1^6 = 1 &\equiv 1 \bmod 8, \\ 3^6 = 729 &\equiv 1 \bmod 8, \\ 5^6 \equiv (-3)^6 = 3^6 &\equiv 1 \bmod 8, \\ 7^6 \equiv (-1)^6 = 1^6 &\equiv 1 \bmod 8. \end{aligned}$$

Mooduli 9 suhtes tuleb läbi vaadata jäägid $1,2,4,5,7,8$:

$$\begin{aligned} 1^6 = 1 &\equiv 1 \bmod 9, \\ 2^6 = 64 &\equiv 1 \bmod 9, \\ 4^6 = 2^{12} = (2^6)^2 &\equiv 1^2 \equiv 1 \bmod 9, \\ 5^6 \equiv (-4)^6 = 4^6 &\equiv 1 \bmod 9, \\ 7^6 \equiv (-2)^6 = 2^6 &\equiv 1 \bmod 9, \\ 8^6 \equiv (-1)^6 = 1^6 &\equiv 1 \bmod 9. \end{aligned}$$

Oleme kõikvõimalikud jäägid läbi vaadanud ja vastava 6. astme jääk on alati 1.

19.21 Vastus: ainus võimalus on $m = 4$, $n = 1$.

Kui $m = 1$, saame võrrandi $1 - n = 3$, mille lahend $n = -2$ pole positiivne. Kui $n = 1$, saame võrrandi $m - 1 = 3$, kust tuleb lahend $m = 4$. Edasi võime seega vaadelda juhtu $m, n \geqslant 2$.

Kõigepealt paneme tähele, et kui m ja n oleksid sama paarsusega, oleks avaldise $m^n - n^m$ väärtus paarisarv. Seega peavad m ja n olema erineva paarsusega.

Uurime ülesannde avaldise jääki jagamisel 8-ga ning vaatame selleks läbi kaks juhtu.

Kui m on paaris ja n paaritu, saame eeldusest $n \geqslant 2$ muuhulgas, et $n \geqslant 3$. Järelikult $m^n \equiv 0 \bmod 8$.

Teisest küljest annab paaritu arvu ruut 8-ga jagamisel jäägi 1. Selles saame veenduda näiteks jääkide uurimise põhiprintsiibi alusel, vaadates läbi võimalikud paaritud jäägid, mis 8-ga jagamisel tekkida võivad:

$$\begin{aligned} 1^2 = 1 &= 1 \bmod 8, \\ 3^2 = 9 &= 1 \bmod 8, \\ 5^2 = 25 &= 1 \bmod 8, \\ 7^2 = 49 &= 1 \bmod 8. \end{aligned}$$

Teine võimalus on panna tähele, et $(2k+1)^2 = 4k(k+1) + 1$. Kuna järjestikustest arvudest k ja $k+1$ täpselt üks on paaris, jagub avaldis $4k(k+1)$ kindlasti 8-ga, mistõttu annab $4k(k+1) + 1$ arvuga 8 jagades jäägi 1 (vt ka ülesannet 22.2).

Niisiis $n^2 \equiv 1 \bmod 8$, millest omakorda järeldub $n^m \equiv 1 \bmod 8$ ja kokkuvõttes $m^n - n^m \equiv 7 \bmod 8$.

Kui aga m on paaritu ja n paaris, saame analoogiliselt, et $m^n - n^m \equiv 1 \bmod 8$. Kummalgi juhul pole võimalik tulemuseks saada arvu 3.

19.22 Vastus: jah.

Proovides läbi väikeseid n-i väärtusi, leiame, et

$$\begin{aligned} 2^{2^2-1} - 7 &= 1 = 1^2, \\ 2^{2^3-1} - 7 &= 121 = 11^2, \\ 2^{2^4-1} - 7 &= 32761 = 181^2. \end{aligned}$$

Osutub, et $n = 5$ korral pole aga $2^{2^5-1} - 7 = 2^{31} - 7$ täisruut. Selle tõestamiseks piisab leida moodul, mille järgi $2^{31} - 7$ ei anna ühegi täisruuduga sama jääki.

Vähimaks niisuguseks mooduliks on 11. Paneme tähele, et kehtib kongruents $2^5 = 32 \equiv -1 \bmod 11$, järelikult

$$2^{31} = 2^{30} \cdot 2 = (2^5)^6 \cdot 2 \equiv (-1)^6 \cdot 2 = 1 \cdot 2 = 2 \bmod 11$$

ja

$$2^{31} - 7 \equiv 2 - 7 = -5 \equiv 6 \bmod 11\,.$$

Jääb tõestada, et ükski täisruut ei saa 11-ga jagades anda jääki 6. Selles saame veenduda näiteks jääkide uurimise põhiprintsiibi alusel, vaadates läbi kõik arvud $0, 1, \ldots, 10$:

$$\begin{aligned}
0^2 &= 0 \equiv 0 \bmod 11\,,\\
1^2 &= 1 \equiv 1 \bmod 11\,,\\
2^2 &= 4 \equiv 4 \bmod 11\,,\\
3^2 &= 9 \equiv 9 \bmod 11\,,\\
4^2 &= 16 \equiv 5 \bmod 11\,,\\
5^2 &= 25 \equiv 3 \bmod 11\,,\\
6^2 \equiv (-5)^2 &= 5^2 \equiv 3 \bmod 11\,,\\
7^2 \equiv (-4)^2 &= 4^2 \equiv 5 \bmod 11\,,\\
8^2 \equiv (-3)^2 &= 3^2 \equiv 9 \bmod 11\,,\\
9^2 \equiv (-2)^2 &= 2^2 \equiv 4 \bmod 11\,,\\
10^2 \equiv (-1)^2 &= 1^2 \equiv 1 \bmod 11\,.
\end{aligned}$$

Võrdust $2^{10} \equiv 1 \bmod 11$ saab lihtsalt tõestada Fermat' väikese teoreemi abil. Tegelikult võimaldavad Fermat' väike teoreem ja Euleri teoreem seda ülesannet lahendada ka teistel viisidel, vt ülesannet 25.6.

19.23 Paneme tähele, et

$$3^n + 3^{n+1} + \ldots + 3^{2n} = 3^n(1 + 3 + 3^2 + \ldots + 3^n)\,.$$

Arvud 3^n ja $1 + 3 + 3^2 + \ldots + 3^n$ on ühistegurita, järelikult peavad nad mõlemad olema täisruudud. Selleks, et 3^n oleks täisruut, peab n olema paaris.

Jääb veel tõestada, et paarisarvulise n väärtuse korral saab $1 + 3 + 3^2 + \ldots + 3^n$ olla täisruut ainult siis, kui $n \vdots 4$.

Vaatleme paarisarvu n, mis ei jagu 4-ga, st $n \equiv 2 \bmod 4$. Otsime niisugust moodulit, mille järgi avaldis $1 + 3 + 3^2 + \ldots + 3^n$ annaks sellise jäägi, mida ei saa anda ükski täisruut. Kuidas säärast moodulit leida?

Kuna vaadeldaval juhul $n \equiv 2 \bmod 4$, tasub uurida, kuidas käitub avu 3 nelja järjestikuse astme summa. Paneme tähele, et iga naturaalarvu m jaoks

$$3^m + 3^{m+1} + 3^{m+2} + 3^{m+3} = 3^m(1 + 3 + 3^2 + 3^3) = 3^m \cdot 40\,.$$

Järelikult kui k jagub 4-ga, jagub arvu 3 iga k järjestikuse astme summa 40-ga. Muuhulgas saame

$$1 + 3 + 3^2 + 3^3 + \ldots + 3^n \equiv 1 + 3 + 3^2 = 13 \bmod 40\,,$$

sest summa $3^3 + \ldots + 3^n$ liidetavate arv jagub 4-ga, kui $n \equiv 2 \bmod 4$.

Jääb üle veenduda, et ükski täisruut ei saa 40-ga jagades anda jääki 13. Jääkide uurimise põhiprintsiipi otse rakendades tuleks läbi vaadata 40 jääki $0, 1, \ldots, 39$, aga saab ka kavalamalt. Näiteks võime tähele panna, et kui summa $S \equiv 13 \bmod 40$, siis muuhulgas $S \equiv 3 \bmod 5$.

Nüüd piisab jääkide uurimise põhiprintsiibi abil veenduda, et ükski täisruut ei anna 5-ga jagades jääki 3. Selleks vaatame läbi arvude $0, 1, \ldots, 4$ ruutude jäägid jagamisel 5-ga:

$$\begin{aligned} 0^2 = 0 &\equiv 0 \bmod 5, \\ 1^2 = 1 &\equiv 1 \bmod 5, \\ 2^2 = 4 &\equiv 4 \bmod 5, \\ 3^2 = 9 &\equiv 4 \bmod 5, \\ 4^2 = 16 &\equiv 1 \bmod 5. \end{aligned}$$

Sama moodi annab vastuolu moodul 8, sest $S \equiv 5 \bmod 8$, aga ainsad jäägid, mis saavad tekkida täisruudu jagamisel 8-ga on 0, 1 ja 4.

Lisaks on huvitav tähele panna, et kui $n = 0$ ja $n = 4$, tuleb ülesande avaldise väärtus tõepoolest täisruut, vastavalt siis $1 = 1^2$ ja $9801 = 99^2$.

19.24 Vastus: a) ei, b) ei.

Ülesande mõlemas osas on lahenduse võtmeks leida "halb" moodul, mille järgi vastav võrdus kehtida ei saa.

a)-osas on kohe näha, et moodul 2 ei tööta, sest kui x ja y on mõlemad paaritud, siis on seda ka avaldis $x^2 - xy + y^2$. Äkki sobib moodul 3? Koostame jääkide uurimise põhiprintsiibi alusel 3×3 tabeli, kuhu arvutame uuritava avaldise jäägid 3 järgi, kui x ja y võtavad kõikvõimalikud väärtused hulgast $\{0, 1, 2\}$.

	0	1	2
0	0	1	1
1	1	1	0
2	1	0	1

Näeme, et jääki 2 ei teki. Et aga $2021 \equiv 2 \bmod 3$, pole uuritava avaldise väärtusena arvu 2021 võimalik saada.

b)-osas moodul 2 jälle ei tööta (vastuolu ei tule näiteks siis, kui x ja y on mõlemad paaris). Kuna $2022 \equiv 0 \bmod 3$, ei sobi vastuolu saamiseks ka moodul 3. Proovime moodulit 4 ja koostame avaldise $x^2 - xy + y^2$ jääkide tabeli.

	0	1	2	3
0	0	1	0	1
1	1	1	3	3
2	0	3	0	3
3	1	3	3	1

Näeme taas, et jääki 2 ei teki. Et aga $2022 \equiv 2 \bmod 4$, pole uuritava avaldise väärtusena võimalik saada ka arvu 2022.

19.25 Kui b on paaritu, annavad nii b^4 kui ka b^2 paaritute täisruutudena 4-ga jagamisel jäägi 1. Arvu $3b^2$ jääk jagamisel 4-ga on järelikult 3 ja kogu summa $b^4 + 3b^2 + 4$

jääk jagamisel 4-ga on 0 ehk $b^4+3b^2+4 \vdots 4$. Teisest küljest on selge, et kui b on paarisarv, siis samuti $b^4+3b^2+4 \vdots 4$. Niisiis jagub antud murru nimetaja alati 4-ga.

Kuna murru väärtus on täisarv, peab ka tema lugeja 4-ga jaguma. Paarituarvulise a korral annavad nii a^2 kui a^4, aga järelikult ka $5a^4$ jagamisel 4-ga jäägi 1, mistõttu $5a^4+a^2 \equiv 2 \bmod 4$. See tähendab, et antud murru lugeja jaguks 2-ga, aga mitte 4-ga.

Niisiis peab a olema positiivne paarisarv. Ainus võimalus, mille puhul ta poleks kordarv, on $a=2$. Siis $5a^4+a^2=84$. Jääb üle kontrollida, et kui $b=1$ ja $b=2$, siis b^4+3b^2+4 väärtused on vastavalt 8 ja 32, mis kumbki ei jaga arvu 84. Kui aga $b \geqslant 3$, siis $b^4+3b^2+4 \geqslant 81+27+4>84$ ning jälle ei saa ülesande murru väärtuseks tulla täisarv.

19.26 Vastus: 1 ja 49.

Jääkide uurimise põhiprintsiip võimaldab anda sellele ülesandele kontseptuaalselt lihtsa lahenduse. Piisab, kui vaatame hulgast $\{1,2,\ldots,119\}$ läbi kõik väärtused r, mis on 120-ga ühistegurita, ning leiame nende ruutude jäägid 120-ga jagamisel.

Paraku jääb niisugune lahendus pikaks (sobivaid väärtusi on 32) ning veaohtlikuks (suurim neist väärtustest on 119). Kas me suudame seda lahendust kuidagi lihtsustada? Õnneks jah.

Paneme kõigepealt tähele, et arv r on ühistegurita arvuga $120=2^3\cdot 3\cdot 5$ parajasti siis, kui ta on ühistegurita arvuga $60=2^2\cdot 3\cdot 5$. Suvaline 120-ga ühistegurita arv avaldub seega kujul $60a+b$ mingite täisarvude a ja b korral, kus $\text{SÜT}(b,60)=1$. Samas paneme tähele, et

$$(60a+b)^2 = 3600a^2+120ab+b^2 = 120\cdot(30a^2+ab)+b^2 \equiv b^2 \bmod 120.$$

Niisiis piisab, kui vaatame hulgast $\{1,2,\ldots,59\}$ läbi kõik väärtused b, mis on 60-ga ühistegurita, ning leiame nende ruutude jäägid 120-ga jagamisel. Paraku on ka neid arve veel üpris palju (nimelt 16) ja suurim neist on 59. Kas me saame vajalikku töö hulka veel kuidagi vähendada?

Järgmine mõte on proovida moodulit 30, sest suvaline arv r on ühistegurita arvuga $120=2^3\cdot 3\cdot 5$ parajasti siis, kui ta on ühistegurita ka arvuga $30=2\cdot 3\cdot 5$. Iga 120-ga ühistegurita arv avaldub seega kujul $30c+d$ mingite täisarvude c ja d korral, kus $\text{SÜT}(d,30)=1$. Uurime selle avaldise ruutu:

$$(30c+d)^2 = 900c^2+60cd+d^2.$$

Kuna $900 \not\vdots 120$ ja $60 \not\vdots 120$, tundub korraks, et oleme tupikus. Õnneks osutub, et isegi juhul, kui arvud $900c^2$ ja $60cd$ eraldivõetuna 120-ga ei jagu, teeb nende summa seda ometigi. Eraldame avaldisest $900c^2$ kindlalt 120-ga jaguva osa:

$$900c^2+60cd+d^2 = 840c^2+60c^2+60cd+d^2 = 7\cdot 120c^2+60c(c+d)+d^2.$$

Kui c on paarisarv, saame kohe, et $60c(c+d) \vdots 120$. Kui c on aga paaritu, paneme tähele, et ka d peab olema paaritu, sest ta on 30-ga ühistegurita. Niisiis on $c+d$ paarisarv ja jälle $60c(c+d) \vdots 120$. Järelikult kehtib ka $(30c+d)^2 \equiv d^2 \bmod 120$.

Seega piisab tegelikult, kui vaatame hulgast $\{1,2,\ldots,29\}$ läbi kõik väärtused d, mis on 30-ga ühistegurita, ning leiame nende ruutude jäägid 120-ga jagamisel.

Niisuguseid väärusi on ainult kaheksa ning nende läbivaatamine on juba üsna lihtne:

$$\begin{aligned}
1^2 = 1 &\equiv 1 \bmod 120,\\
7^2 = 49 &\equiv 49 \bmod 120,\\
11^2 = 121 &\equiv 1 \bmod 120,\\
13^2 = 169 &\equiv 49 \bmod 120,\\
17^2 = 289 &\equiv 49 \bmod 120,\\
19^2 = 361 &\equiv 1 \bmod 120,\\
23^2 = 529 &\equiv 49 \bmod 120,\\
29^2 = 841 &\equiv 1 \bmod 120.
\end{aligned}$$

Näeme, et tekivad ainult jäägid 1 ja 49.

19.27 Geomeetrilise jada summa valemist (või valemist (11.1)) teame, et

$$\frac{b^n-1}{b-1} = b^{n-1} + b^{n-2} + \ldots + b + 1.$$

Uurime selle avaldise käitumist mooduli 8 järgi.

Kuna b on paarisarv, siis $b^k \equiv 0 \bmod 8$, kui $k \geqslant 3$. Järelikult

$$\frac{b^n-1}{b-1} \equiv b+1 \bmod 8, \quad \text{kui } n=2, \quad \text{ja} \quad \frac{b^n-1}{b-1} \equiv b^2+b+1 \bmod 8, \quad \text{kui } n \geqslant 3.$$

Igal juhul on $\dfrac{b^n-1}{b-1}$ paaritu, niisiis saab ta olla ainult paaritu arvu ruut. Paaritute arvude ruudud aga saavad 8-ga jagades anda ainult jäägi 1 (vaata näiteks ülesannete 22.2 ja 19.21 lahendusi).

Kui $n=2$, saame $b+1 \equiv 1 \bmod 8$, millest järeldub kohe $b \vdots 8$. Kui aga aga $n \geqslant 3$, saame $b^2+b+1 \equiv 1 \bmod 8$, millest omakorda $b^2+b \vdots 8$. Kuna $b^2+b = b(b+1)$ ja $b+1$ on paaritu, peab ka sel korral kehtima $b \vdots 8$.

Viimases väites saame loomulikult veenduda ka võimalikke jääke läbi vaadates. Paarisarv võib 8-ga jagades anda jäägi $0, 2, 4$ või 6. Nendel juhtudel saame

$$\begin{aligned}
0^2 + 0 + 1 = 1 &\equiv 1 \bmod 8,\\
2^2 + 2 + 1 = 7 &\equiv 7 \bmod 8,\\
4^2 + 4 + 1 = 21 &\equiv 5 \bmod 8,\\
6^2 + 6 + 1 = 43 &\equiv 3 \bmod 8.
\end{aligned}$$

Näeme, et ainult jääk 0 annab uuritava avaldise jäägiks 1, seega on $b \vdots 8$ ainus võimalus.