

Arvuteooriast

Lauri Tart

Ülevaade

Arvuteooria

Algarvud

Algarvud ja aritmeetilised jadad

Algarvude jaotus

Algarvuvaalemeid

Aditiivsest arvuteooriast

Ülevaade

Arvuteooria

Algarvud

Algarvud ja aritmeetilised jadad

Algarvude jaotus

Algarvuvaalemeid

Aditiivsest arvuteooriast

Arvuteooria on matemaatika haru, mis uurib täisarvude ja nendega seotud matemaatiliste objektide (nt. ratsionaalarvud, Gaussi täisarvud, täisarvuliste kordajatega võrrandite abil defineeritud kõverad, Turingi masinad) omadusi.

Arvuteooria võib tinglikult jagada järgmisteks alamharudeks:

- ▶ **algebra**line arvuteooria: täisarvude üldistuste (algebraised arvud) poolt moodustatud algebraiste struktuuride uurimine;
- ▶ **analüütiline** arvuteooria: täisarvude uurimine kas reaal- ja kompleksmuutuja funktsioonide teooria abil või nende suuruse ja jaotuse alusel või mõlemat korraga;
- ▶ diofantiline või aritmeetiline **geomeetria**: täisarvuliste kordajatega võrrandite uurimine kõverate ja pindade terminites;
- ▶ **tõenäosuslik** arvuteooria: arvuteoreetiliste küsimuste uurimine tõenäosusteooria vahenditega;
- ▶ aritmeetiline **kombinatorika**: aritmeetiliste tehetega seotud kombinatoorsed hinnangud, sealhulgas aditiivne arvuteooria;
- ▶ **arvutuslik** arvuteooria: täisarvudel töötavad algoritmid, nende kiirus ja võimalikkus.

Arvuteooria võib tinglikult jagada järgmisteks alamharudeks:

- ▶ **algebra**line arvuteooria: täisarvude üldistuste (algebraised arvud) poolt moodustatud algebraiste struktuuride uurimine;
- ▶ **analüütiline** arvuteooria: täisarvude uurimine kas reaal- ja kompleksmuutuja funktsioonide teooria abil või nende suuruse ja jaotuse alusel või mõlemat korraga;
- ▶ diofantiline või aritmeetiline **geomeetria**: täisarvuliste kordajatega võrrandite uurimine kõverate ja pindade terminites;
- ▶ **tõenäosuslik** arvuteooria: arvuteoreetiliste küsimuste uurimine tõenäosusteooria vahenditega;
- ▶ aritmeetiline **kombinatorika**: aritmeetiliste tehetega seotud kombinatoorsed hinnangud, sealhulgas aditiivne arvuteooria;
- ▶ **arvutuslik** arvuteooria: täisarvudel töötavad algoritmid, nende kiirus ja võimalikkus.

Arvuteooria võib tinglikult jagada järgmisteks alamharudeks:

- ▶ **algebra**line arvuteooria: täisarvude üldistuste (algebralised arvud) poolt moodustatud algebraliste struktuuride uurimine;
- ▶ **analüütiline** arvuteooria: täisarvude uurimine kas reaal- ja kompleksmuutuja funktsioonide teooria abil või nende suuruse ja jaotuse alusel või mõlemat korraga;
- ▶ diofantiline või aritmeetiline **geomeetria**: täisarvuliste kordajatega võrrandite uurimine kõverate ja pindade terminites;
- ▶ **tõenäosuslik** arvuteooria: arvuteoreetiliste küsimuste uurimine tõenäosusteooria vahenditega;
- ▶ aritmeetiline **kombinatorika**: aritmeetiliste tehetega seotud kombinatoorsed hinnangud, sealhulgas aditiivne arvuteooria;
- ▶ **arvutuslik** arvuteooria: täisarvudel töötavad algoritmid, nende kiirus ja võimalikkus.

Arvuteooria võib tinglikult jagada järgmisteks alamharudeks:

- ▶ **algebra**line arvuteooria: täisarvude üldistuste (algebralised arvud) poolt moodustatud algebraliste struktuuride uurimine;
- ▶ **analüütiline** arvuteooria: täisarvude uurimine kas reaali- ja kompleksmuutuja funktsioonide teooria abil või nende suuruse ja jaotuse alusel või mõlemat korraga;
- ▶ diofantiline või aritmeetiline **geomeetria**: täisarvuliste kordajatega võrrandite uurimine kõverate ja pindade terminites;
- ▶ **tõenäosuslik** arvuteooria: arvuteoreetiliste küsimuste uurimine tõenäosusteooria vahenditega;
- ▶ aritmeetiline **kombinatorika**: aritmeetiliste tehetega seotud kombinatoorsed hinnangud, sealhulgas aditiivne arvuteooria;
- ▶ **arvutuslik** arvuteooria: täisarvudel töötavad algoritmid, nende kiirus ja võimalikkus.

Arvuteooria võib tinglikult jagada järgmisteks alamharudeks:

- ▶ **algebra**line arvuteooria: täisarvude üldistuste (algebralised arvud) poolt moodustatud algebraliste struktuuride uurimine;
- ▶ **analüütiline** arvuteooria: täisarvude uurimine kas reaali- ja kompleksmuutuja funktsioonide teooria abil või nende suuruse ja jaotuse alusel või mõlemat korraga;
- ▶ diofantiline või aritmeetiline **geomeetria**: täisarvuliste kordajatega võrrandite uurimine kõverate ja pindade terminites;
- ▶ **tõenäosuslik** arvuteooria: arvuteoreetiliste küsimuste uurimine tõenäosusteooria vahenditega;
- ▶ aritmeetiline **kombinatorika**: aritmeetiliste tehetega seotud kombinatoorsed hinnangud, sealhulgas aditiivne arvuteooria;
- ▶ **arvutuslik** arvuteooria: täisarvudel töötavad algoritmid, nende kiirus ja võimalikkus.

Arvuteooria võib tinglikult jagada järgmisteks alamharudeks:

- ▶ **algebra**line arvuteooria: täisarvude üldistuste (algebralised arvud) poolt moodustatud algebraliste struktuuride uurimine;
- ▶ **analüütiline** arvuteooria: täisarvude uurimine kas reaal- ja kompleksmuutuja funktsioonide teooria abil või nende suuruse ja jaotuse alusel või mõlemat korraga;
- ▶ diofantiline või aritmeetiline **geomeetria**: täisarvuliste kordajatega võrrandite uurimine kõverate ja pindade terminites;
- ▶ **tõenäosuslik** arvuteooria: arvuteoreetiliste küsimuste uurimine tõenäosusteooria vahenditega;
- ▶ aritmeetiline **kombinatorika**: aritmeetiliste tehetega seotud kombinatoorsed hinnangud, sealhulgas aditiivne arvuteooria;
- ▶ **arvutuslik** arvuteooria: täisarvudel töötavad algoritmid, nende kiirus ja võimalikkus.

Arvuteooria võib tinglikult jagada järgmisteks alamharudeks:

- ▶ **algebra**line arvuteooria: täisarvude üldistuste (algebralised arvud) poolt moodustatud algebraliste struktuuride uurimine;
- ▶ **analüütiline** arvuteooria: täisarvude uurimine kas reaali- ja kompleksmuutuja funktsioonide teooria abil või nende suuruse ja jaotuse alusel või mõlemat korraga;
- ▶ diofantiline või aritmeetiline **geomeetria**: täisarvuliste kordajatega võrrandite uurimine kõverate ja pindade terminites;
- ▶ **tõenäosuslik** arvuteooria: arvuteoreetiliste küsimuste uurimine tõenäosusteooria vahenditega;
- ▶ aritmeetiline **kombinatorika**: aritmeetiliste tehetega seotud kombinatoorsed hinnangud, sealhulgas aditiivne arvuteooria;
- ▶ **arvutuslik** arvuteooria: täisarvudel töötavad algoritmid, nende kiirus ja võimalikkus.

Ülevaade

Arvuteooria

Algarvud

Algarvud ja aritmeetilised jadad

Algarvude jaotus

Algarvuvaalemeid

Aditiivsest arvuteooriast

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

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

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

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

Definitsioon 1

Täisarvu $n > 1$ nimetatakse *algarvuks*, kui ta ei ole esitatav kujul $n = a \cdot b$, kus $1 < a, b < n$. Täisarvu $n > 1$, mis ei ole algarv, nimetatakse *kordarvuks*.

Üks põhjusi, miks algarvud on olulised, on vast kõigile koolist tuttav:

Teoreem 1 (Aritmeetika põhiteoreem)

Iga naturaalarvu $n > 1$ saab esitada *algarvude korrutisena* (s.t. leiduvad $r \in \mathbb{N}$ ja algarvud $p_1, \dots, p_r$ nii, et $n = p_1 \dots p_r$) ning see esitus on *ühene* tegurite järjekorra täpsuseni.

Seega algarvud on nii-öelda naturaalarvude “ehituskivid”, kus “ehitamine” tähendab korrutamist. Algarve p_i nimetatakse arvu n *algteguriteks* ja korrutist $p_1 \dots p_r$ kutsutakse arvu n *algteguriteks lahutuseks*.

Definitsioon 1

Täisarvu $n > 1$ nimetatakse *algarvuks*, kui ta ei ole esitatav kujul $n = a \cdot b$, kus $1 < a, b < n$. Täisarvu $n > 1$, mis ei ole algarv, nimetatakse *kordarvuks*.

Üks põhjusi, miks algarvud on olulised, on vast kõigile koolist tuttav:

Teoreem 1 (Aritmeetika põhiteoreem)

Iga naturaalarvu $n > 1$ saab esitada *algarvude korrutisena* (s.t. leiduvad $r \in \mathbb{N}$ ja algarvud $p_1, \dots, p_r$ nii, et $n = p_1 \dots p_r$) ning see esitus on *ühene* tegurite järjekorra täpsuseni.

Seega algarvud on nii-öelda naturaalarvude “ehituskivid”, kus “ehitamine” tähendab korrutamist. Algarve p_i nimetatakse arvu n *algteguriteks* ja korrutist $p_1 \dots p_r$ kutsutakse arvu n *algteguriteks lahutuseks*.

Definitsioon 1

Täisarvu $n > 1$ nimetatakse *algarvuks*, kui ta ei ole esitatav kujul $n = a \cdot b$, kus $1 < a, b < n$. Täisarvu $n > 1$, mis ei ole algarv, nimetatakse *kordarvuks*.

Üks põhjusi, miks algarvud on olulised, on vast kõigile koolist tuttav:

Teoreem 1 (Aritmeetika põhiteoreem)

Iga naturaalarvu $n > 1$ saab esitada *algarvude korrutisena* (s.t. leiduvad $r \in \mathbb{N}$ ja algarvud $p_1, \dots, p_r$ nii, et $n = p_1 \dots p_r$) ning see esitus on *ühene* tegurite järjekorra täpsuseni.

Seega algarvud on nii-öelda naturaalarvude “ehituskivid”, kus “ehitamine” tähendab korrutamist. Algarve p_i nimetatakse arvu n *algteguriteks* ja korrutist $p_1 \dots p_r$ kutsutakse arvu n *algteguriteks lahutuseks*.

Definitsioon 1

Täisarvu $n > 1$ nimetatakse *algarvuks*, kui ta ei ole esitatav kujul $n = a \cdot b$, kus $1 < a, b < n$. Täisarvu $n > 1$, mis ei ole algarv, nimetatakse *kordarvuks*.

Üks põhjusi, miks algarvud on olulised, on vast kõigile koolist tuttav:

Teoreem 1 (Aritmeetika põhiteoreem)

Iga naturaalarvu $n > 1$ saab esitada *algarvude korrutisena* (s.t. leiduvad $r \in \mathbb{N}$ ja algarvud $p_1, \dots, p_r$ nii, et $n = p_1 \dots p_r$) ning see esitus on *ühene* tegurite järjekorra täpsuseni.

Seega algarvud on nii-öelda naturaalarvude “ehituskivid”, kus “ehitamine” tähendab korrutamist. Algarve p_i nimetatakse arvu n *algteguriteks* ja korrutist $p_1 \dots p_r$ kutsutakse arvu n *algteguriteks lahutuseks*.

Juba vanakreeka matemaatik Eukleides teadis, et algarve on väga palju.

Teoreem 2 (Eukleides)

Algarvude hulk on lõpmatu.

Tõestus: Olgu kõiki algarve lõplik arv ja nummerdame need järjest ära: $p_1, p_2, p_3, \dots, p_n$. Siis p_n on kõige suurem algarv. Vaatleme sellist arvu:

$$a = p_1 p_2 \dots p_n + 1 > p_n.$$

Kuna eelduse kohaselt on tegu kordarvuga, siis aritmeetika põhiteoreemi tõttu leidub tal algarvuline tegur p_i kõigi algarvude hulgast $\{p_1, p_2, p_3, \dots, p_n\}$. Seega p_i jagab arvu a ja ilmselt ka arvu $p_1 p_2 \dots p_n$. Järelikult jagab p_i ka vahet $a - p_1 p_2 \dots p_n = 1$, mis on võimatu.

Juba vanakreeka matemaatik Eukleides teadis, et algarve on väga palju.

Teoreem 2 (Eukleides)

Algarvude hulk on lõpmatu.

Tõestus: Olgu kõiki algarve lõplik arv ja nummerdame need järjest ära: $p_1, p_2, p_3, \dots, p_n$. Siis p_n on kõige suurem algarv. Vaatleme sellist arvu:

$$a = p_1 p_2 \dots p_n + 1 > p_n.$$

Kuna eelduse kohaselt on tegu kordarvuga, siis aritmeetika põhiteoreemi tõttu leidub tal algarvuline tegur p_i kõigi algarvude hulgast $\{p_1, p_2, p_3, \dots, p_n\}$. Seega p_i jagab arvu a ja ilmselt ka arvu $p_1 p_2 \dots p_n$. Järelikult jagab p_i ka vahet $a - p_1 p_2 \dots p_n = 1$, mis on võimatu.

Juba vanakreeka matemaatik Eukleides teadis, et algarve on väga palju.

Teoreem 2 (Eukleides)

Algarvude hulk on lõpmatu.

Tõestus: Olgu kõiki algarve lõplik arv ja nummerdame need järjest ära: $p_1, p_2, p_3, \dots, p_n$. Siis p_n on kõige suurem algarv. Vaatleme sellist arvu:

$$a = p_1 p_2 \dots p_n + 1 > p_n.$$

Kuna eelduse kohaselt on tegu kordarvuga, siis aritmeetika põhiteoreemi tõttu leidub tal algarvuline tegur p_i kõigi algarvude hulgast $\{p_1, p_2, p_3, \dots, p_n\}$. Seega p_i jagab arvu a ja ilmselt ka arvu $p_1 p_2 \dots p_n$. Järelikult jagab p_i ka vahet $a - p_1 p_2 \dots p_n = 1$, mis on võimatu.

Juba vanakreeka matemaatik Eukleides teadis, et algarve on väga palju.

Teoreem 2 (Eukleides)

Algarvude hulk on lõpmatu.

Tõestus: Olgu kõiki algarve lõplik arv ja nummerdame need järjest ära: $p_1, p_2, p_3, \dots, p_n$. Siis p_n on kõige suurem algarv. Vaatleme sellist arvu:

$$a = p_1 p_2 \dots p_n + 1 > p_n.$$

Kuna eelduse kohaselt on tegu kordarvuga, siis aritmeetika põhiteoreemi tõttu leidub tal algarvuline tegur p_i kõigi algarvude hulgast $\{p_1, p_2, p_3, \dots, p_n\}$. Seega p_i jagab arvu a ja ilmselt ka arvu $p_1 p_2 \dots p_n$. Järelikult jagab p_i ka vahet $a - p_1 p_2 \dots p_n = 1$, mis on võimatu.

Juba vanakreeka matemaatik Eukleides teadis, et algarve on väga palju.

Teoreem 2 (Eukleides)

Algarvude hulk on lõpmatu.

Tõestus: Olgu kõiki algarve lõplik arv ja nummerdame need järjest ära: $p_1, p_2, p_3, \dots, p_n$. Siis p_n on kõige suurem algarv. Vaatleme sellist arvu:

$$a = p_1 p_2 \dots p_n + 1 > p_n.$$

Kuna eelduse kohaselt on tegu kordarvuga, siis aritmeetika põhiteoreemi tõttu leidub tal algarvuline tegur p_i kõigi algarvude hulgast $\{p_1, p_2, p_3, \dots, p_n\}$. Seega p_i jagab arvu a ja ilmselt ka arvu $p_1 p_2 \dots p_n$. Järelikult jagab p_i ka vahet $a - p_1 p_2 \dots p_n = 1$, mis on võimatu.

Aritmeetika põhiteoreemist tulenevalt on mõned olulised algarvudega seotud küsimused järgmised

- ▶ leida etteantud arvu n lahutus algteguriteks,
- ▶ teha kindlaks, kas etteantud arv p on algarv,
- ▶ leida kõik algarvud mingis vahemikus.
- ▶ leida võimalikult suur algarv.

Suurim tänaseks teadaolev algarv on pärineb aastast 2013 ja selleks on $2^{57885161} - 1$. Algarve kujul $2^n - 1$ nimetatakse **Mersenne'i** algarvudeks. Kümme suurimat teadaolevat algarvu on Mersenne'i algarvud, sest meetodid kujul $2^n - 1$ olevate arvude algarvulisuse kontrolliks on teadaolevatest kiireimad.

Näiteks mitmed tänapäevase elektroonilise side aspektid toetuvad asjaolule, et suurte arvude korral ei ole keegi suutnud neid probleeme väga **kiiresti** lahendada (v.a. kvantarvutite abil).

Aritmeetika põhiteoreemist tulenevalt on mõned olulised algarvudega seotud küsimused järgmised

- ▶ leida etteantud arvu n lahutus algteguriteks,
- ▶ teha kindlaks, kas etteantud arv p on algarv,
- ▶ leida kõik algarvud mingis vahemikus.
- ▶ leida võimalikult suur algarv.

Suurim tänaseks teadaolev algarv on pärineb aastast 2013 ja selleks on $2^{57885161} - 1$. Algarve kujul $2^n - 1$ nimetatakse Mersenne'i algarvudeks. Kümme suurimat teadaolevat algarvu on Mersenne'i algarvud, sest meetodid kujul $2^n - 1$ olevate arvude algarvulisuse kontrolliks on teadaolevatest kiireimad.

Näiteks mitmed tänapäevase elektroonilise side aspektid toetuvad asjaolule, et suurte arvude korral ei ole keegi suutnud neid probleeme väga kiiresti lahendada (v.a. kvantarvutite abil).

Aritmeetika põhiteoreemist tulenevalt on mõned olulised algarvudega seotud küsimused järgmised

- ▶ leida etteantud arvu n lahutus algteguriteks,
- ▶ teha kindlaks, kas etteantud arv p on algarv,
- ▶ leida kõik algarvud mingis vahemikus.
- ▶ leida võimalikult suur algarv.

Suurim tänaseks teadaolev algarv on pärineb aastast 2013 ja selleks on $2^{57885161} - 1$. Algarve kujul $2^n - 1$ nimetatakse Mersenne'i algarvudeks. Kümme suurimat teadaolevat algarvu on Mersenne'i algarvud, sest meetodid kujul $2^n - 1$ olevate arvude algarvulisuse kontrolliks on teadaolevatest kiireimad.

Näiteks mitmed tänapäevase elektroonilise side aspektid toetuvad asjaolule, et suurte arvude korral ei ole keegi suutnud neid probleeme väga kiiresti lahendada (v.a. kvantarvutite abil).

Aritmeetika põhiteoreemist tulenevalt on mõned olulised algarvudega seotud küsimused järgmised

- ▶ leida etteantud arvu n lahutus algteguriteks,
- ▶ teha kindlaks, kas etteantud arv p on algarv,
- ▶ leida kõik algarvud mingis vahemikus.
- ▶ leida võimalikult suur algarv.

Suurim tänaseks teadaolev algarv on pärineb aastast 2013 ja selleks on $2^{57885161} - 1$. Algarve kujul $2^n - 1$ nimetatakse Mersenne'i algarvudeks. Kümme suurimat teadaolevat algarvu on Mersenne'i algarvud, sest meetodid kujul $2^n - 1$ olevate arvude algarvulisuse kontrolliks on teadaolevatest kiireimad.

Näiteks mitmed tänapäevase elektroonilise side aspektid toetuvad asjaolule, et suurte arvude korral ei ole keegi suutnud neid probleeme väga kiiresti lahendada (v.a. kvantarvutite abil).

Aritmeetika põhiteoreemist tulenevalt on mõned olulised algarvudega seotud küsimused järgmised

- ▶ leida etteantud arvu n lahutus algteguriteks,
- ▶ teha kindlaks, kas etteantud arv p on algarv,
- ▶ leida kõik algarvud mingis vahemikus.
- ▶ leida võimalikult suur algarv.

Suurim tänaseks teadaolev algarv on pärineb aastast 2013 ja selleks on $2^{57885161} - 1$. Algarve kujul $2^n - 1$ nimetatakse Mersenne'i algarvudeks. Kümme suurimat teadaolevat algarvu on Mersenne'i algarvud, sest meetodid kujul $2^n - 1$ olevate arvude algarvulisuse kontrolliks on teadaolevatest kiireimad.

Näiteks mitmed tänapäevase elektroonilise side aspektid toetuvad asjaolule, et suurte arvude korral ei ole keegi suutnud neid probleeme väga kiiresti lahendada (v.a. kvantarvutite abil).

Aritmeetika põhiteoreemist tulenevalt on mõned olulised algarvudega seotud küsimused järgmised

- ▶ leida etteantud arvu n lahutus algteguriteks,
- ▶ teha kindlaks, kas etteantud arv p on algarv,
- ▶ leida kõik algarvud mingis vahemikus.
- ▶ leida võimalikult suur algarv.

Suurim tänaseks teadaolev algarv on pärineb aastast 2013 ja selleks on $2^{57885161} - 1$. Algarve kujul $2^n - 1$ nimetatakse Mersenne'i algarvudeks. Kümme suurimat teadaolevat algarvu on Mersenne'i algarvud, sest meetodid kujul $2^n - 1$ olevate arvude algarvulisuse kontrolliks on teadaolevatest kiireimad.

Näiteks mitmed tänapäevase elektroonilise side aspektid toetuvad asjaolule, et suurte arvude korral ei ole keegi suutnud neid probleeme väga kiiresti lahendada (v.a. kvantarvutite abil).

Aritmeetika põhiteoreemist tulenevalt on mõned olulised algarvudega seotud küsimused järgmised

- ▶ leida etteantud arvu n lahutus algteguriteks,
- ▶ teha kindlaks, kas etteantud arv p on algarv,
- ▶ leida kõik algarvud mingis vahemikus.
- ▶ leida võimalikult suur algarv.

Suurim tänaseks teadaolev algarv on pärineb aastast 2013 ja selleks on $2^{57885161} - 1$. Algarve kujul $2^n - 1$ nimetatakse **Mersenne'i** algarvudeks. Kümme suurimat teadaolevat algarvu on Mersenne'i algarvud, sest meetodid kujul $2^n - 1$ olevate arvude algarvulisuse kontrolliks on teadaolevatest kiireimad.

Näiteks mitmed tänapäevase elektroonilise side aspektid toetuvad asjaolule, et suurte arvude korral ei ole keegi suutnud neid probleeme väga **kiiresti** lahendada (v.a. kvantarvutite abil).

Aritmeetika põhiteoreemist tulenevalt on mõned olulised algarvudega seotud küsimused järgmised

- ▶ leida etteantud arvu n lahutus algteguriteks,
- ▶ teha kindlaks, kas etteantud arv p on algarv,
- ▶ leida kõik algarvud mingis vahemikus.
- ▶ leida võimalikult suur algarv.

Suurim tänaseks teadaolev algarv on pärineb aastast 2013 ja selleks on $2^{57885161} - 1$. Algarve kujul $2^n - 1$ nimetatakse Mersenne'i algarvudeks. Kümme suurimat teadaolevat algarvu on Mersenne'i algarvud, sest meetodid kujul $2^n - 1$ olevate arvude algarvulisuse kontrolliks on teadaolevatest kiireimad.

Näiteks mitmed tänapäevase elektroonilise side aspektid toetuvad asjaolule, et suurte arvude korral ei ole keegi suutnud neid probleeme väga kiiresti lahendada (v.a. kvantarvutite abil).

Aritmeetika põhiteoreemist tulenevalt on mõned olulised algarvudega seotud küsimused järgmised

- ▶ leida etteantud arvu n lahutus algteguriteks,
- ▶ teha kindlaks, kas etteantud arv p on algarv,
- ▶ leida kõik algarvud mingis vahemikus.
- ▶ leida võimalikult suur algarv.

Suurim tänaseks teadaolev algarv on pärineb aastast 2013 ja selleks on $2^{57885161} - 1$. Algarve kujul $2^n - 1$ nimetatakse Mersenne'i algarvudeks. Kümme suurimat teadaolevat algarvu on Mersenne'i algarvud, sest meetodid kujul $2^n - 1$ olevate arvude algarvulisuse kontrolliks on teadaolevatest kiireimad.

Näiteks mitmed tänapäevase elektroonilise side aspektid toetuvad asjaolule, et suurte arvude korral ei ole keegi suutnud neid probleeme väga kiiresti lahendada (v.a. kvantarvutite abil).

Üks arvutuslikult kiiremaid algarvulisuse kontrollimise meetodeid tugineb järgmisele tuntud arvuteooria tulemusele.

Teoreem 3 (Fermat' väike teoreem)

Kui p on algarv ja a on täisarv, mis ei jagu arvuga p , siis

$$\frac{a^{p-1} - 1}{p}$$

on täisarv, ehk kongruentside keeles

$$a^{p-1} \equiv 1 \pmod{p}.$$

Üks arvutuslikult kiiremaid algarvulisuse kontrollimise meetodeid tugineb järgmisele tuntud arvuteooria tulemusele.

Teoreem 3 (Fermat' väike teoreem)

Kui p on algarv ja a on täisarv, mis ei jagu arvuga p , siis

$$\frac{a^{p-1} - 1}{p}$$

on täisarv, ehk kongruentside keeles

$$a^{p-1} \equiv 1 \pmod{p}.$$

Test ise on järgmine.

- ▶ Sisendiks on naturaalarv n .
- ▶ Valime vabalt sellise täisarvu $1 < a < n$, mis ei jagu arvuga n .
- ▶ Kui $\frac{a^{n-1}-1}{n}$ ei ole täisarv, siis n on kordarv.
- ▶ Vastasel juhul valime uue a väärtuse vahemikust $[2, n-1]$ ja kordame protsessi.
- ▶ Üldiselt on kordarvu n korral vähemalt pooled a võimalikest väärtustest sellised, et $\frac{a^{n-1}-1}{n}$ ei ole täisarv.
- ▶ Järelikult mitme erineva a väärtusega testides võime väita, et n on tõenäoliselt algarv.

Test ise on järgmine.

- ▶ Sisendiks on naturaalarv n .
- ▶ Valime vabalt sellise täisarvu $1 < a < n$, mis ei jagu arvuga n .
- ▶ Kui $\frac{a^{n-1}-1}{n}$ ei ole täisarv, siis n on kordarv.
- ▶ Vastasel juhul valime uue a väärtuse vahemikust $[2, n-1]$ ja kordame protsessi.
- ▶ Üldiselt on kordarvu n korral vähemalt pooled a võimalikest väärtustest sellised, et $\frac{a^{n-1}-1}{n}$ ei ole täisarv.
- ▶ Järelikult mitme erineva a väärtusega testides võime väita, et n on tõenäoliselt algarv.

Test ise on järgmine.

- ▶ Sisendiks on naturaalarv n .
- ▶ Valime vabalt sellise täisarvu $1 < a < n$, mis ei jagu arvuga n .
- ▶ Kui $\frac{a^{n-1}-1}{n}$ ei ole täisarv, siis n on kordarv.
- ▶ Vastasel juhul valime uue a väärtuse vahemikust $[2, n-1]$ ja kordame protsessi.
- ▶ Üldiselt on kordarvu n korral vähemalt pooled a võimalikest väärtustest sellised, et $\frac{a^{n-1}-1}{n}$ ei ole täisarv.
- ▶ Järelikult mitme erineva a väärtusega testides võime väita, et n on tõenäoliselt algarv.

Test ise on järgmine.

- ▶ Sisendiks on naturaalarv n .
- ▶ Valime vabalt sellise täisarvu $1 < a < n$, mis ei jagu arvuga n .
- ▶ Kui $\frac{a^{n-1}-1}{n}$ ei ole täisarv, siis n on kordarv.
- ▶ Vastasel juhul valime uue a väärtuse vahemikust $[2, n-1]$ ja kordame protsessi.
- ▶ Üldiselt on kordarvu n korral vähemalt pooled a võimalikest väärtustest sellised, et $\frac{a^{n-1}-1}{n}$ ei ole täisarv.
- ▶ Järelikult mitme erineva a väärtusega testides võime väita, et n on tõenäoliselt algarv.

Test ise on järgmine.

- ▶ Sisendiks on naturaalarv n .
- ▶ Valime vabalt sellise täisarvu $1 < a < n$, mis ei jagu arvuga n .
- ▶ Kui $\frac{a^{n-1}-1}{n}$ ei ole täisarv, siis n on kordarv.
- ▶ Vastasel juhul valime uue a väärtuse vahemikust $[2, n-1]$ ja kordame protsessi.
- ▶ Üldiselt on kordarvu n korral vähemalt pooled a võimalikest väärtustest sellised, et $\frac{a^{n-1}-1}{n}$ ei ole täisarv.
- ▶ Järelikult mitme erineva a väärtusega testides võime väita, et n on tõenäoliselt algarv.

Test ise on järgmine.

- ▶ Sisendiks on naturaalarv n .
- ▶ Valime vabalt sellise täisarvu $1 < a < n$, mis ei jagu arvuga n .
- ▶ Kui $\frac{a^{n-1}-1}{n}$ ei ole täisarv, siis n on kordarv.
- ▶ Vastasel juhul valime uue a väärtuse vahemikust $[2, n-1]$ ja kordame protsessi.
- ▶ Üldiselt on kordarvu n korral vähemalt pooled a võimalikest väärtustest sellised, et $\frac{a^{n-1}-1}{n}$ ei ole täisarv.
- ▶ Järelikult mitme erineva a väärtusega testides võime väita, et n on tõenäoliselt algarv.

Test ise on järgmine.

- ▶ Sisendiks on naturaalarv n .
- ▶ Valime vabalt sellise täisarvu $1 < a < n$, mis **ei jagu** arvuga n .
- ▶ Kui $\frac{a^{n-1}-1}{n}$ ei ole täisarv, siis n on **kordarv**.
- ▶ Vastasel juhul valime uue a väärtuse vahemikust $[2, n-1]$ ja kordame protsessi.
- ▶ **Üldiselt** on kordarvu n korral **vähemalt pooled** a võimalikest väärtustest sellised, et $\frac{a^{n-1}-1}{n}$ ei ole täisarv.
- ▶ Järelikult mitme erineva a väärtusega testides võime väita, et n on **tõenäoliselt algarv**.

Võib muidugi juhtuda, et me juhuslikult valime ainult neid arvu a väärtusi, mille korral $\frac{a^{n-1}-1}{n}$ on täisarv, aga arv n ise on kordarv.

Samuti võib arv n olla üks sellistest võrdlemisi harvaesinevatest kordarvudest (nn. Carmichaeli arvud), mille korral peaaegu kõigi a väärtuste korral on $\frac{a^{n-1}-1}{n}$ täisarv.

Seega Fermat' algarvulisuse test ei ole 100% kindel, aga see-eest on ta väga kiire ja selle läbinud arve võib mõne teise, põhjalikuma testiga üle kontrollida.

Võib muidugi juhtuda, et me juhuslikult valime ainult neid arvu a väärtusi, mille korral $\frac{a^{n-1}-1}{n}$ on täisarv, aga arv n ise on kordarv.

Samuti võib arv n olla üks sellistest võrdlemisi harvaesinevatest kordarvudest (nn. Carmichaeli arvud), mille korral peaaegu kõigi a väärtuste korral on $\frac{a^{n-1}-1}{n}$ täisarv.

Seega Fermat' algarvulisuse test ei ole 100% kindel, aga see-eest on ta väga kiire ja selle läbinud arve võib mõne teise, põhjalikuma testiga üle kontrollida.

Võib muidugi juhtuda, et me juhuslikult valime ainult neid arvu a väärtusi, mille korral $\frac{a^{n-1}-1}{n}$ on täisarv, aga arv n ise on kordarv.

Samuti võib arv n olla üks sellistest võrdlemisi harvaesinevatest kordarvudest (nn. Carmichaeli arvud), mille korral peaaegu kõigi a väärtuste korral on $\frac{a^{n-1}-1}{n}$ täisarv.

Seega Fermat' algarvulisuse test ei ole 100% kindel, aga see-eest on ta väga kiire ja selle läbinud arve võib mõne teise, põhjalikuma testiga üle kontrollida.

Ülevaade

Arvuteooria

Algarvud

Algarvud ja aritmeetilised jadad

Algarvude jaotus

Algarvuvaalemeid

Aditiivsest arvuteooriast

Olgu meil antud aritmeetiline jada, näiteks

3, 8, 13, 18, 23, 28, 33, 38, 43, 48, 53, 58

Arvuteooriast huvitatud inimesele pakub sel juhul kohe huvi küsimus: kui palju algarve ja kordarve selles jadas on?

Kordarvud:

3, 8, 13, 18, 23, 28, 33, 38, 43, 48, 53, 58

Neid ilmselt **lõpmata** palju.

Algarvud:

3, 8, 13, 18, 23, 28, 33, 38, 43, 48, 53, 58

Neid on tegelikult ka **lõpmata** palju.

Olgu meil antud aritmeetiline jada, näiteks

3, 8, 13, 18, 23, 28, 33, 38, 43, 48, 53, 58

Arvuteooriast huvitatud inimesele pakub sel juhul kohe huvi küsimus: kui palju algarve ja kordarve selles jadas on?

Kordarvud:

3, 8, 13, 18, 23, 28, 33, 38, 43, 48, 53, 58

Neid ilmselt lõpmata palju.

Algarvud:

3, 8, 13, 18, 23, 28, 33, 38, 43, 48, 53, 58

Neid on tegelikult ka lõpmata palju.

Olgu meil antud aritmeetiline jada, näiteks

3, 8, 13, 18, 23, 28, 33, 38, 43, 48, 53, 58

Arvuteooriast huvitatud inimesele pakub sel juhul kohe huvi küsimus: kui palju algarve ja kordarve selles jadas on?

Kordarvud:

3, 8, 13, 18, 23, 28, 33, 38, 43, 48, 53, 58

Neid ilmselt **lõpmata** palju.

Algarvud:

3, 8, 13, 18, 23, 28, 33, 38, 43, 48, 53, 58

Neid on tegelikult ka **lõpmata** palju.

Olgu meil antud aritmeetiline jada, näiteks

3, 8, 13, 18, 23, 28, 33, 38, 43, 48, 53, 58

Arvuteooriast huvitatud inimesele pakub sel juhul kohe huvi küsimus: kui palju algarve ja kordarve selles jadas on?

Kordarvud:

3, 8, 13, 18, 23, 28, 33, 38, 43, 48, 53, 58

Neid ilmselt **lõpmata** palju.

Algarvud:

3, 8, 13, 18, 23, 28, 33, 38, 43, 48, 53, 58

Neid on tegelikult ka **lõpmata** palju.

Olgu meil antud aritmeetiline jada, näiteks

3, 8, 13, 18, 23, 28, 33, 38, 43, 48, 53, 58

Arvuteooriast huvitatud inimesele pakub sel juhul kohe huvi küsimus: kui palju algarve ja kordarve selles jadas on?

Kordarvud:

3, 8, 13, 18, 23, 28, 33, 38, 43, 48, 53, 58

Neid ilmselt **lõpmata** palju.

Algarvud:

3, 8, 13, 18, 23, 28, 33, 38, 43, 48, 53, 58

Neid on tegelikult ka **lõpmata** palju.

Veelgi üldisemalt, millised kombinatsioonid algarvudest ja kordarvudest üldse võivad aritmeetilises jadas esineda?

- ▶ Mitte ühtegi algarvu, nt. 4, 8, 12, 16, 20, ...
- ▶ Lõplik arv algarve, nt. 2, 6, 10, 14, 18, 22, ...
- ▶ Lõpmata palju algarve, nt. 1, 2, 3, 4, 5, 6, 7, ...
- ▶ Lõpmata palju kordarve.

Viimane juhtum esineb tegelikult **kõigis** aritmeetilistes jadades.

Lause 1

Igas aritmeetilises jadas $(a + kb)_{k=1}^{\infty}$ on lõpmata palju kordarve, näiteks

$$a(1 + b), a(1 + 2b), a(1 + 3b), \dots$$

Veelgi üldisemalt, millised kombinatsioonid algarvudest ja kordarvudest üldse võivad aritmeetilises jadas esineda?

- ▶ Mitte ühtegi algarvu, nt. 4, 8, 12, 16, 20, ...
- ▶ Lõplik arv algarve, nt. 2, 6, 10, 14, 18, 22, ...
- ▶ Lõpmata palju algarve, nt. 1, 2, 3, 4, 5, 6, 7, ...
- ▶ Lõpmata palju kordarve.

Viimane juhtum esineb tegelikult **kõigis** aritmeetilistes jadades.

Lause 1

Igas aritmeetilises jadas $(a + kb)_{k=1}^{\infty}$ on lõpmata palju kordarve, näiteks

$$a(1 + b), a(1 + 2b), a(1 + 3b), \dots$$

Veelgi üldisemalt, millised kombinatsioonid algarvudest ja kordarvudest üldse võivad aritmeetilises jadas esineda?

- ▶ Mitte ühtegi algarvu, nt. 4, 8, 12, 16, 20, ...
- ▶ Lõplik arv algarve, nt. 2, 6, 10, 14, 18, 22, ...
- ▶ Lõpmata palju algarve, nt. 1, 2, 3, 4, 5, 6, 7, ...
- ▶ Lõpmata palju kordarve.

Viimane juhtum esineb tegelikult **kõigis** aritmeetilistes jadades.

Lause 1

Igas aritmeetilises jadas $(a + kb)_{k=1}^{\infty}$ on lõpmata palju kordarve, näiteks

$$a(1 + b), a(1 + 2b), a(1 + 3b), \dots$$

Veelgi üldisemalt, millised kombinatsioonid algarvudest ja kordarvudest üldse võivad aritmeetilises jadas esineda?

- ▶ Mitte ühtegi algarvu, nt. 4, 8, 12, 16, 20,
- ▶ Lõplik arv algarve, nt. 2, 6, 10, 14, 18, 22,
- ▶ Lõpmata palju algarve, nt. 1, 2, 3, 4, 5, 6, 7,
- ▶ Lõpmata palju kordarve.

Viimane juhtum esineb tegelikult **kõigis** aritmeetilistes jadades.

Lause 1

Igas aritmeetilises jadas $(a + kb)_{k=1}^{\infty}$ on lõpmata palju kordarve, näiteks

$$a(1 + b), a(1 + 2b), a(1 + 3b), \dots$$

Veelgi üldisemalt, millised kombinatsioonid algarvudest ja kordarvudest üldse võivad aritmeetilises jadas esineda?

- ▶ Mitte ühtegi algarvu, nt. 4, 8, 12, 16, 20,
- ▶ Lõplik arv algarve, nt. 2, 6, 10, 14, 18, 22,
- ▶ Lõpmata palju algarve, nt. 1, 2, 3, 4, 5, 6, 7,
- ▶ Lõpmata palju kordarve.

Viimane juhtum esineb tegelikult **kõigis** aritmeetilistes jadades.

Lause 1

Igas aritmeetilises jadas $(a + kb)_{k=1}^{\infty}$ on lõpmata palju kordarve, näiteks

$$a(1 + b), a(1 + 2b), a(1 + 3b), \dots$$

Veelgi üldisemalt, millised kombinatsioonid algarvudest ja kordarvudest üldse võivad aritmeetilises jadas esineda?

- ▶ Mitte ühtegi algarvu, nt. 4, 8, 12, 16, 20,
- ▶ Lõplik arv algarve, nt. 2, 6, 10, 14, 18, 22,
- ▶ Lõpmata palju algarve, nt. 1, 2, 3, 4, 5, 6, 7,
- ▶ Lõpmata palju kordarve.

Viimane juhtum esineb tegelikult **kõigis** aritmeetilistes jadades.

Lause 1

Igas aritmeetilises jadas $(a + kb)_{k=1}^{\infty}$ on lõpmata palju kordarve, näiteks

$$a(1 + b), a(1 + 2b), a(1 + 3b), \dots$$

Veelgi üldisemalt, millised kombinatsioonid algarvudest ja kordarvudest üldse võivad aritmeetilises jadas esineda?

- ▶ Mitte ühtegi algarvu, nt. 4, 8, 12, 16, 20, ...
- ▶ Lõplik arv algarve, nt. 2, 6, 10, 14, 18, 22, ...
- ▶ Lõpmata palju algarve, nt. 1, 2, 3, 4, 5, 6, 7, ...
- ▶ Lõpmata palju kordarve.

Viimane juhtum esineb tegelikult **kõigis** aritmeetilistes jadades.

Lause 1

Igas aritmeetilises jadas $(a + kb)_{k=1}^{\infty}$ on lõpmata palju kordarve, näiteks

$$a(1 + b), a(1 + 2b), a(1 + 3b), \dots$$

Lõpmata paljude **algarvude** leidumist aritmeetilises jadas käsitleb järgmine, analüütilise arvuteooria valda kuuluv tulemus.

Teoreem 4 (Dirichlet)

Kui a ja b on naturaalarvud ja $S\ddot{U}T(a, b) = 1$, siis aritmeetilises jadas

$$a, a + b, a + 2b, a + 3b, \dots$$

on lõpmata palju algarve. Fikseeritud täisarvu b korral on kõigis jadades

$$a_i, a_i + b, a_i + 2b, a_i + 3b, \dots$$

ligikaudu sama palju algarve, kus $1 \leq a_i \leq b$ ja $S\ddot{U}T(a, b) = 1$.

Lõpmata paljude **algarvude** leidumist aritmeetilises jadas käsitleb järgmine, analüütilise arvuteooria valda kuuluv tulemus.

Teoreem 4 (Dirichlet)

Kui a ja b on naturaalarvud ja $S\ddot{U}T(a, b) = 1$, siis aritmeetilises jadas

$$a, a + b, a + 2b, a + 3b, \dots$$

on lõpmata palju algarve. Fikseeritud täisarvu b korral on kõigis jadades

$$a_i, a_i + b, a_i + 2b, a_i + 3b, \dots$$

ligikaudu sama palju algarve, kus $1 \leq a_i \leq b$ ja $S\ddot{U}T(a, b) = 1$.

Lõpmata paljude **algarvude** leidumist aritmeetilises jadas käsitleb järgmine, analüütilise arvuteooria valda kuuluv tulemus.

Teoreem 4 (Dirichlet)

Kui a ja b on naturaalarvud ja $S\ddot{U}T(a, b) = 1$, siis aritmeetilises jadas

$$a, a + b, a + 2b, a + 3b, \dots$$

on lõpmata palju algarve. Fikseeritud täisarvu b korral on kõigis jadades

$$a_i, a_i + b, a_i + 2b, a_i + 3b, \dots$$

ligikaudu sama palju algarve, kus $1 \leq a_i \leq b$ ja $S\ddot{U}T(a, b) = 1$.

Teiselt poolt, äkki ei taha me mitte uurida seda, kas mingis jadas on algarve, vaid tahame algarvudest moodustada võimalikult **pikki** aritmeetilisi jadasid.

Tuleb välja, et on võimalik konstrueerida kuitahes pikki **ainult algarvudest** koosnevaid algarvulisi jadasid. Näiteks

3, 5, 7,

5, 11, 17, 23, 29

121 174 811, 121 174 841, 121 174 871, 121 174 901, 121 174 931, 121 174 961,

Seda garanteerib järgmine, aastal 2004. tõestatud tulemus.

Teoreem 5 (Green, Tao)

Iga naturaalarvu n korral leidub n algarvust koosnev aritmeetiline jada.

Teiselt poolt, äkki ei taha me mitte uurida seda, kas mingis jadas on algarve, vaid tahame algarvudest moodustada võimalikult **pikki** aritmeetilisi jadasid.

Tuleb välja, et on võimalik konstrueerida kuitahes pikki **ainult algarvudest** koosnevaid algarvulisi jadasid. Näiteks

3, 5, 7,

5, 11, 17, 23, 29

121 174 811, 121 174 841, 121 174 871, 121 174 901, 121 174 931, 121 174 961,

Seda garanteerib järgmine, aastal 2004. tõestatud tulemus.

Teoreem 5 (Green, Tao)

Iga naturaalarvu n korral leidub n algarvust koosnev aritmeetiline jada.

Teiselt poolt, äkki ei taha me mitte uurida seda, kas mingis jadas on algarve, vaid tahame algarvudest moodustada võimalikult **pikki** aritmeetilisi jadasid.

Tuleb välja, et on võimalik konstrueerida kuitahes pikki **ainult algarvudest** koosnevaid algarvulisi jadasid. Näiteks

3, 5, 7,

5, 11, 17, 23, 29

121 174 811, 121 174 841, 121 174 871, 121 174 901, 121 174 931, 121 174 961,

Seda garanteerib järgmine, aastal 2004. tõestatud tulemus.

Teoreem 5 (Green, Tao)

Iga naturaalarvu n korral leidub n algarvust koosnev aritmeetiline jada.

Teiselt poolt, äkki ei taha me mitte uurida seda, kas mingis jadas on algarve, vaid tahame algarvudest moodustada võimalikult **pikki** aritmeetilisi jadasid.

Tuleb välja, et on võimalik konstrueerida kuitahes pikki **ainult algarvudest** koosnevaid algarvulisi jadasid. Näiteks

3, 5, 7,

5, 11, 17, 23, 29

121 174 811, 121 174 841, 121 174 871, 121 174 901, 121 174 931, 121 174 961,

Seda garanteerib järgmine, aastal 2004. tõestatud tulemus.

Teoreem 5 (Green, Tao)

Iga naturaalarvu n korral leidub n algarvust koosnev aritmeetiline jada.

Teiselt poolt, äkki ei taha me mitte uurida seda, kas mingis jadas on algarve, vaid tahame algarvudest moodustada võimalikult **pikki** aritmeetilisi jadasid.

Tuleb välja, et on võimalik konstrueerida kuitahes pikki **ainult algarvudest** koosnevaid algarvulisi jadasid. Näiteks

3, 5, 7,

5, 11, 17, 23, 29

121 174 811, 121 174 841, 121 174 871, 121 174 901, 121 174 931, 121 174 961,

Seda garanteerib järgmine, aastal 2004. tõestatud tulemus.

Teoreem 5 (Green, Tao)

Iga naturaalarvu n korral leidub n algarvust koosnev aritmeetiline jada.

Teiselt poolt, äkki ei taha me mitte uurida seda, kas mingis jadas on algarve, vaid tahame algarvudest moodustada võimalikult **pikki** aritmeetilisi jadasid.

Tuleb välja, et on võimalik konstrueerida kuitahes pikki **ainult algarvudest** koosnevaid algarvulisi jadasid. Näiteks

3, 5, 7,

5, 11, 17, 23, 29

121 174 811, 121 174 841, 121 174 871, 121 174 901, 121 174 931, 121 174 961,

Seda garanteerib järgmine, aastal 2004. tõestatud tulemus.

Teoreem 5 (Green, Tao)

Iga naturaalarvu n korral leidub n algarvust koosnev aritmeetiline jada.

Ülevaade

Arvuteooria

Algarvud

Algarvud ja aritmeetilised jadad

Algarvude jaotus

Algarvuvaalemeid

Aditiivsest arvuteooriast

Kui algarvude paiknemist uurida, siis on keeruline kohe mingisugust seaduspära näha:

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

Siiski on algarvude paiknemise kohta tehtud mitmeid olulisi tähelepanekuid:

Teoreem 6 (Bertrandi postulaat)

Kui $n > 3$ on naturaalarv, siis n ja $2n - 2$ vahel leidub vähemalt üks algarv.

Lause 2

Iga naturaalarvu n korral leidub n järjestikust kordarvu, näiteks

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

Teoreem 7 (Algarvude asümptootiline jaotus)

Kui $\pi(n)$ tähistab kõigi arvust n väiksemate algarvude arvu, siis kehtib seos

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{n / \ln(n)} = 1 \quad \text{ehk} \quad \pi(n) \approx \frac{n}{\ln n}.$$

Siiski on algarvude paiknemise kohta tehtud mitmeid olulisi tähelepanekuid:

Teoreem 6 (Bertrandi postulaat)

Kui $n > 3$ on naturaalarv, siis n ja $2n - 2$ vahel leidub vähemalt üks algarv.

Lause 2

Iga naturaalarvu n korral leidub n järjestikust kordarvu, näiteks

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

Teoreem 7 (Algarvude asümptootiline jaotus)

Kui $\pi(n)$ tähistab kõigi arvust n väiksemate algarvude arvu, siis kehtib seos

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{n / \ln(n)} = 1 \quad \text{ehk} \quad \pi(n) \approx \frac{n}{\ln n}.$$

Siiski on algarvude paiknemise kohta tehtud mitmeid olulisi tähelepanekuid:

Teoreem 6 (Bertrandi postulaat)

Kui $n > 3$ on naturaalarv, siis n ja $2n - 2$ vahel leidub vähemalt üks algarv.

Lause 2

Iga naturaalarvu n korral leidub n järjestikust kordarvu, näiteks

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

Teoreem 7 (Algarvude asümptootiline jaotus)

Kui $\pi(n)$ tähistab kõigi arvust n väiksemate algarvude arvu, siis kehtib seos

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{n / \ln(n)} = 1 \quad \text{ehk} \quad \pi(n) \approx \frac{n}{\ln n}.$$

Siiski on algarvude paiknemise kohta tehtud mitmeid olulisi tähelepanekuid:

Teoreem 6 (Bertrandi postulaat)

Kui $n > 3$ on naturaalarv, siis n ja $2n - 2$ vahel leidub vähemalt üks algarv.

Lause 2

Iga naturaalarvu n korral leidub n järjestikust kordarvu, näiteks

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

Teoreem 7 (Algarvude asümptootiline jaotus)

Kui $\pi(n)$ tähistab kõigi arvust n väiksemate algarvude arvu, siis kehtib seos

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{n / \ln(n)} = 1 \quad \text{ehk} \quad \pi(n) \approx \frac{n}{\ln n}.$$

Siiski on algarvude paiknemise kohta tehtud mitmeid olulisi tähelepanekuid:

Teoreem 6 (Bertrandi postulaat)

Kui $n > 3$ on naturaalarv, siis n ja $2n - 2$ vahel leidub vähemalt üks algarv.

Lause 2

Iga naturaalarvu n korral leidub n järjestikust kordarvu, näiteks

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

Teoreem 7 (Algarvude asümptootiline jaotus)

Kui $\pi(n)$ tähistab kõigi arvust n väiksemate algarvude arvu, siis kehtib seos

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{n / \ln(n)} = 1 \quad \text{ehk} \quad \pi(n) \approx \frac{n}{\ln n}.$$

Samuti võib tähele panna, et on olemas teineteisele väga lähedal asuvaid algarve.

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

Kui 2 ja 3 kõrvale jätta, siis selliseid algarvude paare kujul $(p, p + 2)$ nimetatakse **algarvukaksikuteks**.

Samuti võib tähele panna, et on olemas teineteisele väga lähedal asuvaid algarve.

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

Kui 2 ja 3 kõrvale jätta, siis selliseid algarvude paare kujul $(p, p + 2)$ nimetatakse **algarvukaksikuteks**.

Üks arvuteooria suuremaid seni lahendamata küsimusi on, kas algarvukaksikuid on lõpmata palju.

Hüpotees 1 (Algarvukaksikute hüpotees)

Algarvukaksikuid on lõpmata palju.

Oletatakse, et see nii tõepoolest on ja arvutuslikult on leitud järjest suuremaid algarvukaksikute paare. Suurim teadaolev on pärit 2011. aastast:

$$(3\,756\,801\,695\,685 \cdot 2^{666\,669} - 1, 3\,756\,801\,695\,685 \cdot 2^{666\,669} + 1).$$

Prantsuse matemaatik de Polignac üldistas selle hüpoteesi kujule

Hüpotees 2 (Polignac'i hüpotees)

Iga paarisarvu n korral leidub lõpmata palju algarvupaare $(p, p + n)$.

Üks arvuteooria suuremaid seni lahendamata küsimusi on, kas algarvukaksikuid on lõpmata palju.

Hüpotees 1 (Algarvukaksikute hüpotees)

Algarvukaksikuid on lõpmata palju.

Oletatakse, et see nii tõepoolest on ja arvutuslikult on leitud järjest suuremaid algarvukaksikute paare. Suurim teadaolev on pärit 2011. aastast:

$$(3\,756\,801\,695\,685 \cdot 2^{666\,669} - 1, 3\,756\,801\,695\,685 \cdot 2^{666\,669} + 1).$$

Prantsuse matemaatik de Polignac üldistas selle hüpoteesi kujule

Hüpotees 2 (Polignac'i hüpotees)

Iga paarisarvu n korral leidub lõpmata palju algarvupaare $(p, p + n)$.

Üks arvuteooria suuremaid seni lahendamata küsimusi on, kas algarvukaksikuid on lõpmata palju.

Hüpotees 1 (Algarvukaksikute hüpotees)

Algarvukaksikuid on lõpmata palju.

Oletatakse, et see nii tõepoolest on ja arvutuslikult on leitud järjest suuremaid algarvukaksikute paare. Suurim teadaolev on pärit 2011. aastast:

$$(3\,756\,801\,695\,685 \cdot 2^{666\,669} - 1, 3\,756\,801\,695\,685 \cdot 2^{666\,669} + 1).$$

Prantsuse matemaatik de Polignac üldistas selle hüpoteesi kujule

Hüpotees 2 (Polignac'i hüpotees)

Iga paarisarvu n korral leidub lõpmata palju algarvupaare $(p, p + n)$.

Kuigi üldjuhul on see hüpotees samuti lahendamata, näitas aastal 2013 ameerika matemaatik Zhang, et teatud n valiku korral antud antud väide tõepoolest kehtib.

Teoreem 8 (Zhang)

On olemas selline paarisarv $n < 70\,000\,000$, mille korral leidub lõpmata palju algarvupaare kujul $(p, p + n)$.

Ülemist tõket 70 000 000 on pärastpoole vähendatud 246-ni. Teatud eeldustel, mis ei ole ise samuti tõestatud, võib tõke olla isegi vaid 6.

Algarvupaare kujul $(p, p + 4)$ nimetatakse **algarvunõbudeks** ja paare kujul $(p, p + 6)$ **seksikateks algarvudeks**. Seega parimal juhul on arvata, et leidub lõpmata palju seksikaid algarve.

Kuigi üldjuhul on see hüpotees samuti lahendamata, näitas aastal 2013 ameerika matemaatik Zhang, et teatud n valiku korral antud antud väide tõepoolest kehtib.

Teoreem 8 (Zhang)

On olemas selline paarisarv $n < 70\,000\,000$, mille korral leidub lõpmata palju algarvupaare kujul $(p, p + n)$.

Ülemist tõket 70 000 000 on pärastpoole vähendatud 246-ni. Teatud eeldustel, mis ei ole ise samuti tõestatud, võib tõke olla isegi vaid 6.

Algarvupaare kujul $(p, p + 4)$ nimetatakse **algarvunõbudeks** ja paare kujul $(p, p + 6)$ **seksikateks algarvudeks**. Seega parimal juhul on arvata, et leidub lõpmata palju seksikaid algarve.

Kuigi üldjuhul on see hüpotees samuti lahendamata, näitas aastal 2013 ameerika matemaatik Zhang, et teatud n valiku korral antud antud väide tõepoolest kehtib.

Teoreem 8 (Zhang)

On olemas selline paarisarv $n < 70\,000\,000$, mille korral leidub lõpmata palju algarvupaare kujul $(p, p + n)$.

Ülemist tõket 70 000 000 on pärastpoole vähendatud 246-ni. Teatud eeldustel, mis ei ole ise samuti tõestatud, võib tõke olla isegi vaid 6.

Algarvupaare kujul $(p, p + 4)$ nimetatakse **algarvunõbudeks** ja paare kujul $(p, p + 6)$ **seksikateks algarvudeks**. Seega parimal juhul on arvata, et leidub lõpmata palju seksikaid algarve.

Kuigi üldjuhul on see hüpotees samuti lahendamata, näitas aastal 2013 ameerika matemaatik Zhang, et teatud n valiku korral antud antud väide tõepoolest kehtib.

Teoreem 8 (Zhang)

On olemas selline paarisarv $n < 70\,000\,000$, mille korral leidub lõpmata palju algarvupaare kujul $(p, p + n)$.

Ülemist tõket 70 000 000 on pärastpoole vähendatud 246-ni. Teatud eeldustel, mis ei ole ise samuti tõestatud, võib tõke olla isegi vaid 6.

Algarvupaare kujul $(p, p + 4)$ nimetatakse **algarvunõbudeks** ja paare kujul $(p, p + 6)$ **seksikateks algarvudeks**. Seega parimal juhul on arvata, et leidub lõpmata palju seksikaid algarve.

Eelneva võib kokku võtta selliselt:

- ▶ algarvud võivad olla üksteisele väga lähedal (algarvukaksikud),
- ▶ algarvud võivad olla teineteisest väga kaugel ja mistahes kaugus on seejuures saavutatav,
- ▶ etteantud algarvu n korral ei pea siiski järgmist algarvu otsima kaugemalt kui $2n - 2$,
- ▶ n -kohalisi algarve on proportsionaalselt ligikaudu kaks korda rohkem, kui $2n$ -kohalisi algarve,
- ▶ arvatavasti on olemas lõpmata palju seksikaid algarve.

Eelneva võib kokku võtta selliselt:

- ▶ algarvud võivad olla üksteisele **väga lähedal** (algarvukaksikud),
- ▶ algarvud võivad olla teineteisest **väga kaugel** ja mistahes kaugus on seejuures saavutatav,
- ▶ etteantud algarvu n korral ei pea siiski järgmist algarvu otsima kaugemalt kui $2n - 2$,
- ▶ n -kohalisi algarve on proportsionaalselt ligikaudu **kaks** korda rohkem, kui $2n$ -kohalisi algarve,
- ▶ arvatavasti on olemas lõpmata palju seksikaid algarve.

Eelneva võib kokku võtta selliselt:

- ▶ algarvud võivad olla üksteisele **väga lähedal** (algarvukaksikud),
- ▶ algarvud võivad olla teineteisest **väga kaugel** ja mistahes kaugus on seejuures saavutatav,
- ▶ etteantud algarvu n korral ei pea siiski järgmist algarvu otsima kaugemalt kui $2n - 2$,
- ▶ n -kohalisi algarve on proportsionaalselt ligikaudu **kaks** korda rohkem, kui $2n$ -kohalisi algarve,
- ▶ arvatavasti on olemas lõpmata palju seksikaid algarve.

Eelneva võib kokku võtta selliselt:

- ▶ algarvud võivad olla üksteisele **väga lähedal** (algarvukaksikud),
- ▶ algarvud võivad olla teineteisest **väga kaugel** ja mistahes kaugus on seejuures saavutatav,
- ▶ etteantud algarvu n korral ei pea siiski järgmist algarvu otsima kaugemalt kui $2n - 2$,
- ▶ n -kohalisi algarve on proportsionaalselt ligikaudu **kaks** korda rohkem, kui $2n$ -kohalisi algarve,
- ▶ arvatavasti on olemas lõpmata palju seksikaid algarve.

Eelneva võib kokku võtta selliselt:

- ▶ algarvud võivad olla üksteisele väga lähedal (algarvukaksikud),
- ▶ algarvud võivad olla teineteisest väga kaugel ja mistahes kaugus on seejuures saavutatav,
- ▶ etteantud algarvu n korral ei pea siiski järgmist algarvu otsima kaugemalt kui $2n - 2$,
- ▶ n -kohalisi algarve on proportsionaalselt ligikaudu kaks korda rohkem, kui $2n$ -kohalisi algarve,
- ▶ arvatavasti on olemas lõpmata palju seksikaid algarve.

Eelneva võib kokku võtta selliselt:

- ▶ algarvud võivad olla üksteisele **väga lähedal** (algarvukaksikud),
- ▶ algarvud võivad olla teineteisest **väga kaugel** ja mistahes kaugus on seejuures saavutatav,
- ▶ etteantud algarvu n korral ei pea siiski järgmist algarvu otsima kaugemalt kui $2n - 2$,
- ▶ n -kohalisi algarve on proportsionaalselt ligikaudu **kaks** korda rohkem, kui $2n$ -kohalisi algarve,
- ▶ arvatavasti on olemas lõpmata palju seksikaid algarve.

Ülevaade

Arvuteooria

Algarvud

Algarvud ja aritmeetilised jadad

Algarvude jaotus

Algarvuvaalemeid

Aditiivsest arvuteooriast

Tähistame kõik algarvud järjest ära kujul

$$p_1 = 2, p_2 = 3, p_3 = 5, \dots$$

Eelnevast teame, et see jada ei lõpe kunagi ära ja (analüüsi abiga)

$$p_n \approx n \cdot \ln n.$$

See ei ole aga täpne valem.

Läbi aegade on proovitud leida valemeid, mis annaksid tulemuseks kas

- ▶ täpselt kõik algarvud,
- ▶ lõpmata palju erinevaid algarve,
- ▶ kõik algarvud ja mingi hulga kordarve,
- ▶ lõpmata palju algarve ja mingi hulga kordarve.

Tähistame kõik algarvud järjest ära kujul

$$p_1 = 2, p_2 = 3, p_3 = 5, \dots$$

Eelnevast teame, et see jada ei lõpe kunagi ära ja (analüüsi abiga)

$$p_n \approx n \cdot \ln n.$$

See ei ole aga täpne valem.

Läbi aegade on proovitud leida valemeid, mis annaksid tulemuseks kas

- ▶ täpselt kõik algarvud,
- ▶ lõpmata palju erinevaid algarve,
- ▶ kõik algarvud ja mingi hulga kordarve,
- ▶ lõpmata palju algarve ja mingi hulga kordarve.

Tähistame kõik algarvud järjest ära kujul

$$p_1 = 2, p_2 = 3, p_3 = 5, \dots$$

Eelnevast teame, et see jada ei lõpe kunagi ära ja (analüüsi abiga)

$$p_n \approx n \cdot \ln n.$$

See ei ole aga **täpne** valem.

Läbi aegade on proovitud leida valemeid, mis annaksid tulemuseks kas

- ▶ täpselt kõik algarvud,
- ▶ lõpmata palju erinevaid algarve,
- ▶ kõik algarvud ja mingi hulga kordarve,
- ▶ lõpmata palju algarve ja mingi hulga kordarve.

Tähistame kõik algarvud järjest ära kujul

$$p_1 = 2, p_2 = 3, p_3 = 5, \dots$$

Eelnevast teame, et see jada ei lõpe kunagi ära ja (analüüsi abiga)

$$p_n \approx n \cdot \ln n.$$

See ei ole aga **täpne** valem.

Läbi aegade on proovitud leida valemeid, mis annaksid tulemuseks kas

- ▶ täpselt kõik algarvud,
- ▶ lõpmata palju erinevaid algarve,
- ▶ kõik algarvud ja mingi hulga kordarve,
- ▶ lõpmata palju algarve ja mingi hulga kordarve.

Tähistame kõik algarvud järjest ära kujul

$$p_1 = 2, p_2 = 3, p_3 = 5, \dots$$

Eelnevast teame, et see jada ei lõpe kunagi ära ja (analüüsi abiga)

$$p_n \approx n \cdot \ln n.$$

See ei ole aga **täpne** valem.

Läbi aegade on proovitud leida valemeid, mis annaksid tulemuseks kas

- ▶ täpselt kõik algarvud,
- ▶ lõpmata palju erinevaid algarve,
- ▶ kõik algarvud ja mingi hulga kordarve,
- ▶ lõpmata palju algarve ja mingi hulga kordarve.

Tähistame kõik algarvud järjest ära kujul

$$p_1 = 2, p_2 = 3, p_3 = 5, \dots$$

Eelnevast teame, et see jada ei lõpe kunagi ära ja (analüüsi abiga)

$$p_n \approx n \cdot \ln n.$$

See ei ole aga **täpne** valem.

Läbi aegade on proovitud leida valemeid, mis annaksid tulemuseks kas

- ▶ täpselt kõik algarvud,
- ▶ lõpmata palju erinevaid algarve,
- ▶ kõik algarvud ja mingi hulga kordarve,
- ▶ lõpmata palju algarve ja mingi hulga kordarve.

Tähistame kõik algarvud järjest ära kujul

$$p_1 = 2, p_2 = 3, p_3 = 5, \dots$$

Eelnevast teame, et see jada ei lõpe kunagi ära ja (analüüsi abiga)

$$p_n \approx n \cdot \ln n.$$

See ei ole aga **täpne** valem.

Läbi aegade on proovitud leida valemeid, mis annaksid tulemuseks kas

- ▶ täpselt kõik algarvud,
- ▶ lõpmata palju erinevaid algarve,
- ▶ kõik algarvud ja mingi hulga kordarve,
- ▶ lõpmata palju algarve ja mingi hulga kordarve.

Tähistame kõik algarvud järjest ära kujul

$$p_1 = 2, p_2 = 3, p_3 = 5, \dots$$

Eelnevast teame, et see jada ei lõpe kunagi ära ja (analüüsi abiga)

$$p_n \approx n \cdot \ln n.$$

See ei ole aga **täpne** valem.

Läbi aegade on proovitud leida valemeid, mis annaksid tulemuseks kas

- ▶ täpselt kõik algarvud,
- ▶ lõpmata palju erinevaid algarve,
- ▶ kõik algarvud ja mingi hulga kordarve,
- ▶ lõpmata palju algarve ja mingi hulga kordarve.

Üks esimesena proovitud võimalus on algarvude leidmine **polünoom**funktsioonide abil.

Näiteks polünoom $f(x) = x^2 + x + 41$ annab $x = 1, 2, 3, \dots, 39$ korral tulemuseks algarvu, aga $f(40) = 40^2 + 40 + 41 = 41^2$. Kui välja jätta konstantsed polünoomid, sest ilmselt on näiteks $f(x) = 3$ korral ainus tulemus algarv, siis ei olegi võimalik ühemuutuja polünoomide abil vaid algarve saada.

Teoreem 9 (Euler)

Ühegi täisarvuliste kordajatega mittekonstantse ühemuutuja **polünoomi** väärtused **ei ole** kõigi muutuja naturaalarvuliste väärtuste korral **algarvud**.

Veelgi enam, ei ole isegi teada, kas mõne vähemalt teise astme ühemuutuja polünoomi väärtuste seas on **lõpmata** palju algarve.

Üks esimesena proovitud võimalus on algarvude leidmine **polünoom**funktsioonide abil.

Näiteks polünoom $f(x) = x^2 + x + 41$ annab $x = 1, 2, 3, \dots, 39$ korral tulemuseks algarvu, aga $f(40) = 40^2 + 40 + 41 = 41^2$. Kui välja jätta konstantsed polünoomid, sest ilmselt on näiteks $f(x) = 3$ korral ainus tulemus algarv, siis ei olegi võimalik ühemuutuja polünoomide abil vaid algarve saada.

Teoreem 9 (Euler)

Ühegi täisarvuliste kordajatega mittekonstantse ühemuutuja **polünoomi** väärtused **ei ole** kõigi muutuja naturaalarvuliste väärtuste korral **algarvud**.

Veelgi enam, ei ole isegi teada, kas mõne vähemalt teise astme ühemuutuja polünoomi väärtuste seas on **lõpmata** palju algarve.

Üks esimesena proovitud võimalus on algarvude leidmine **polünoom**funktsioonide abil.

Näiteks polünoom $f(x) = x^2 + x + 41$ annab $x = 1, 2, 3, \dots, 39$ korral tulemuseks algarvu, aga $f(40) = 40^2 + 40 + 41 = 41^2$. Kui välja jätta konstantsed polünoomid, sest ilmselt on näiteks $f(x) = 3$ korral ainus tulemus algarv, siis ei olegi võimalik ühemuutuja polünoomide abil vaid algarve saada.

Teoreem 9 (Euler)

*Ühegi täisarvuliste kordajatega mittekonstantse ühemuutuja **polünoomi** väärtused **ei ole** kõigi muutuja naturaalarvuliste väärtuste korral **algarvud**.*

Veelgi enam, ei ole isegi teada, kas mõne vähemalt teise astme ühemuutuja polünoomi väärtuste seas on **lõpmata** palju algarve.

Üks esimesena proovitud võimalus on algarvude leidmine **polünoom**funktsioonide abil.

Näiteks polünoom $f(x) = x^2 + x + 41$ annab $x = 1, 2, 3, \dots, 39$ korral tulemuseks algarvu, aga $f(40) = 40^2 + 40 + 41 = 41^2$. Kui välja jätta konstantsed polünoomid, sest ilmselt on näiteks $f(x) = 3$ korral ainus tulemus algarv, siis ei olegi võimalik ühemuutuja polünoomide abil vaid algarve saada.

Teoreem 9 (Euler)

Ühegi täisarvuliste kordajatega mittekonstantse ühemuutuja **polünoomi** väärtused **ei ole** kõigi muutuja naturaalarvuliste väärtuste korral **algarvud**.

Veelgi enam, ei ole isegi teada, kas mõne vähemalt teise astme ühemuutuja polünoomi väärtuste seas on **lõpmata** palju algarve.

Üks esimesena proovitud võimalus on algarvude leidmine **polünoom**funktsioonide abil.

Näiteks polünoom $f(x) = x^2 + x + 41$ annab $x = 1, 2, 3, \dots, 39$ korral tulemuseks algarvu, aga $f(40) = 40^2 + 40 + 41 = 41^2$. Kui välja jätta konstantsed polünoomid, sest ilmselt on näiteks $f(x) = 3$ korral ainus tulemus algarv, siis ei olegi võimalik ühemuutuja polünoomide abil vaid algarve saada.

Teoreem 9 (Euler)

*Ühegi täisarvuliste kordajatega mittekonstantse ühemuutuja **polünoomi** väärtused **ei ole** kõigi muutuja naturaalarvuliste väärtuste korral **algarvud**.*

Veelgi enam, ei ole isegi teada, kas mõne vähemalt teise astme ühemuutuja polünoomi väärtuste seas on **lõpmata** palju algarve.

Mitmemuutuja polünoomide jaoks see siiski kehtib, näiteks on kõik järgmise 26-muutuja polünoomi **positiivsed** väärtused algarvud:

$$\begin{aligned}
 & f(a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z) \\
 = & (k+2)(1 - [wz + h + j - q]^2 - \\
 & [(gk + 2g + k + 1)(h + j) + h - z]^2 - \\
 & [16(k+1)^3(k+2)(n+1)^2 + 1 - f^2]^2 - \\
 & [2n + p + q + z - e]^2 - [e^3(e+2)(a+1)^2 + 1 - o^2]^2 - \\
 & [(a^2 - 1)y^2 + 1 - x^2]^2 - \\
 & [16r^2y^4(a^2 - 1) + 1 - u^2]^2 - [n + l + v - y]^2 - \\
 & [(a^2 - 1)l^2 + 1 - m^2]^2 - [ai + k + 1 - l - i]^2 - \\
 & [((a + u^2(u^2 - a))^2 - 1)(n + 4dy)^2 + 1 - (x + cu)^2]^2 - \\
 & [p + l(a - n - 1) + b(2an + 2a - n^2 - 2n - 2) - m]^2 - \\
 & [q + y(a - p - 1) + s(2ap + 2a - p^2 - 2p - 2) - x]^2 - \\
 & [z + pl(a - p) + t(2ap - p^2 - 1) - pm]^2).
 \end{aligned}$$

Mitmemuutuja polünoomide jaoks see siiski kehtib, näiteks on kõik järgmise 26-muutuja polünoomi **positiivsed** väärtused algarvud:

$$\begin{aligned}
 & f(a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z) \\
 = & (k + 2)(1 - [wz + h + j - q]^2 - \\
 & [(gk + 2g + k + 1)(h + j) + h - z]^2 - \\
 & [16(k + 1)^3(k + 2)(n + 1)^2 + 1 - f^2]^2 - \\
 & [2n + p + q + z - e]^2 - [e^3(e + 2)(a + 1)^2 + 1 - o^2]^2 - \\
 & [(a^2 - 1)y^2 + 1 - x^2]^2 - \\
 & [16r^2y^4(a^2 - 1) + 1 - u^2]^2 - [n + l + v - y]^2 - \\
 & [(a^2 - 1)l^2 + 1 - m^2]^2 - [ai + k + 1 - l - i]^2 - \\
 & [((a + u^2(u^2 - a))^2 - 1)(n + 4dy)^2 + 1 - (x + cu)^2]^2 - \\
 & [p + l(a - n - 1) + b(2an + 2a - n^2 - 2n - 2) - m]^2 - \\
 & [q + y(a - p - 1) + s(2ap + 2a - p^2 - 2p - 2) - x]^2 - \\
 & [z + pl(a - p) + t(2ap - p^2 - 1) - pm]^2).
 \end{aligned}$$

Samuti on olemas mittepõlünomiaalseid valemeid:

Mills'i valem (1947): leidub reaalarv A nii, et iga naturaalarvu n korral on $\lfloor A^{3^n} \rfloor$ algarv.

Wright'i valem (1951): leidub reaalarv $\omega \approx 1,92878$ nii, et iga naturaalarvu n korral on $\left\lfloor 2^{2^{2^{\cdot^{\cdot^{\cdot^{2^\omega}}}}}} \right\rfloor$ algarv.

Sierpinski'i valem (1952): leidub reaalarv $A \approx 0.02030005$ nii, et

$$p_n = \lfloor 10^{2^n} \cdot A \rfloor - 10^{2^{n-1}} \lfloor 10^{2^{n-1}} \cdot A \rfloor.$$

Willans'i valem (1964): $p_n = 1 + \sum_{k=1}^{2^n} \left\lfloor \sqrt[n]{\frac{n}{1+\pi(k)}} \right\rfloor$.

Samuti on olemas mittepõlünomiaalseid valemeid:

Mills'i valem (1947): leidub reaalarv A nii, et iga naturaalarvu n korral on $\lfloor A^{3^n} \rfloor$ algarv.

Wright'i valem (1951): leidub reaalarv $\omega \approx 1,92878$ nii, et iga naturaalarvu n korral on $\left\lfloor 2^{2^{2^{\cdot^{\cdot^{\cdot^{2^\omega}}}}}} \right\rfloor$ algarv.

Sierpinski'i valem (1952): leidub reaalarv $A \approx 0.02030005$ nii, et

$$p_n = \lfloor 10^{2^n} \cdot A \rfloor - 10^{2^{n-1}} \lfloor 10^{2^{n-1}} \cdot A \rfloor.$$

Willans'i valem (1964): $p_n = 1 + \sum_{k=1}^{2^n} \left\lfloor \sqrt[n]{\frac{n}{1+\pi(k)}} \right\rfloor.$

Samuti on olemas mittepõlünomiaalseid valemeid:

Mills'i valem (1947): leidub reaalarv A nii, et iga naturaalarvu n korral on $\lfloor A^{3^n} \rfloor$ algarv.

Wright'i valem (1951): leidub reaalarv $\omega \approx 1,92878$ nii, et iga naturaalarvu n korral on $\lfloor 2^{2^{2^{\cdot^{\cdot^{\cdot^{2^\omega}}}}}} \rfloor$ algarv.

Sierpinski'i valem (1952): leidub reaalarv $A \approx 0.02030005$ nii, et

$$p_n = \lfloor 10^{2^n} \cdot A \rfloor - 10^{2^{n-1}} \lfloor 10^{2^{n-1}} \cdot A \rfloor.$$

Willans'i valem (1964): $p_n = 1 + \sum_{k=1}^{2^n} \left\lfloor \sqrt[n]{\frac{n}{1+\pi(k)}} \right\rfloor$.

Samuti on olemas mittepõlünomiaalseid valemeid:

Mills'i valem (1947): leidub reaalarv A nii, et iga naturaalarvu n korral on $\lfloor A^{3^n} \rfloor$ algarv.

Wright'i valem (1951): leidub reaalarv $\omega \approx 1,92878$ nii, et iga naturaalarvu n korral on $\left\lfloor 2^{2^{2^{\cdot^{\cdot^{\cdot^{2^\omega}}}}}} \right\rfloor$ algarv.

Sierpinski'i valem (1952): leidub reaalarv $A \approx 0.02030005$ nii, et

$$p_n = \lfloor 10^{2^n} \cdot A \rfloor - 10^{2^{n-1}} \lfloor 10^{2^{n-1}} \cdot A \rfloor.$$

Willans'i valem (1964): $p_n = 1 + \sum_{k=1}^{2^n} \left\lfloor \sqrt[n]{\frac{n}{1+\pi(k)}} \right\rfloor$.

Samuti on olemas mittepõlünomiaalseid valemeid:

Mills'i valem (1947): leidub reaalarv A nii, et iga naturaalarvu n korral on $\lfloor A^{3^n} \rfloor$ algarv.

Wright'i valem (1951): leidub reaalarv $\omega \approx 1,92878$ nii, et iga naturaalarvu n korral on $\left\lfloor 2^{2^{2^{\cdot^{\cdot^{\cdot^{2^\omega}}}}}} \right\rfloor$ algarv.

Sierpinski'i valem (1952): leidub reaalarv $A \approx 0.02030005$ nii, et

$$p_n = \lfloor 10^{2^n} \cdot A \rfloor - 10^{2^{n-1}} \lfloor 10^{2^{n-1}} \cdot A \rfloor.$$

Willans'i valem (1964): $p_n = 1 + \sum_{k=1}^{2^n} \left\lfloor \sqrt[n]{\frac{n}{1+\pi(k)}} \right\rfloor.$

Viimane valem toetub järgmisele arvuteooria tulemusele, millega te saate lähemalt tuttavaks arvuteooria kursuses.

Teoreem 10 (Wilson)

Naturaalarv n on *algarv* siis ja ainult siis, kui $\frac{(n-1)!+1}{n}$ on täisarv, ehk kongruentside keeles

$$(n-1)! \equiv -1 \pmod{n}.$$

Kõigi eeltoodud valemite juures on aga probleemiks see, et *arvutuslikult* on tunduvalt lihtsam kasvõi Eratosthenese sõela abil järjest *kõik algarvud* üles leida. Millisi konstandi jaoks ei ole isegi teada mingit meetodit selle väljaarvutamiseks.

Viimane valem toetub järgmisele arvuteooria tulemusele, millega te saate lähemalt tuttavaks arvuteooria kursuses.

Teoreem 10 (Wilson)

*Naturaalarv n on **algarv** siis ja ainult siis, kui $\frac{(n-1)!+1}{n}$ on täisarv, ehk kongruentside keeles*

$$(n-1)! \equiv -1 \pmod{n}.$$

Kõigi eeltoodud valemite juures on aga probleemiks see, et **arvutuslikult** on tunduvalt lihtsam kasvõi Eratosthenese sõela abil järjest **kõik algarvud** üles leida. Millsi konstandi jaoks ei ole isegi teada mingit meetodit selle väljaarvutamiseks.

Viimane valem toetub järgmisele arvuteooria tulemusele, millega te saate lähemalt tuttavaks arvuteooria kursuses.

Teoreem 10 (Wilson)

*Naturaalarv n on **algarv** siis ja ainult siis, kui $\frac{(n-1)!+1}{n}$ on täisarv, ehk kongruentside keeles*

$$(n-1)! \equiv -1 \pmod{n}.$$

Kõigi eeltoodud valemite juures on aga probleemiks see, et **arvutuslikult** on tunduvalt lihtsam kasvõi Eratosthenese sõela abil järjest **kõik algarvud** üles leida. Millisi konstandi jaoks ei ole isegi teada mingit meetodit selle väljaarvutamiseks.

Ülevaade

Arvuteooria

Algarvud

Algarvud ja aritmeetilised jadad

Algarvude jaotus

Algarvuvaalemeid

Aditiivsest arvuteooriast

Aritmeetika põhiteoreem näitab, et kõik naturaalarvud on esitatavad algarvude korrutistena. Samamoodi on võimalik uurida, milliseid tulemusi võib anda algarvude **liitmine** või liitmine ja korrutamine mingis kombinatsioonis.

Üks kuulsamaid sedasorti küsimusi on tänase päevani lahtine.

Hüpotees 3 (Goldbach)

*Iga paarisarv $n > 2$ on esitatav summana $n = a + b$, kus a ja b on **algarvud**.*

Arvutite abiga on järgi proovitud, et Goldbachi hüpotees kehtib vähemalt suurusjärguni $4 \cdot 10^{18}$, aga tõestust ei ole seni suutnud keegi leida.

Aritmeetika põhiteoreem näitab, et kõik naturaalarvud on esitatavad algarvude korrutistena. Samamoodi on võimalik uurida, milliseid tulemusi võib anda algarvude **liitmine** või liitmine ja korrutamine mingis kombinatsioonis.

Üks kuulsamaid sedasorti küsimusi on tänase päevani lahline.

Hüpotees 3 (Goldbach)

*Iga paarisarv $n > 2$ on esitatav summana $n = a + b$, kus a ja b on **algarvud**.*

Arvutite abiga on järgi proovitud, et Goldbachi hüpotees kehtib vähemalt suurusjärguni $4 \cdot 10^{18}$, aga tõestust ei ole seni suutnud keegi leida.

Aritmeetika põhiteoreem näitab, et kõik naturaalarvud on esitatavad algarvude korrutistena. Samamoodi on võimalik uurida, milliseid tulemusi võib anda algarvude **liitmine** või liitmine ja korrutamine mingis kombinatsioonis.

Üks kuulsamaid sedasorti küsimusi on tänase päevani lahline.

Hüpotees 3 (Goldbach)

*Iga paarisarv $n > 2$ on esitatav summana $n = a + b$, kus a ja b on **algarvud**.*

Arvutite abiga on järgi proovitud, et Goldbachi hüpotees kehtib vähemalt suurusjärguni $4 \cdot 10^{18}$, aga tõestust ei ole seni suutnud keegi leida.

Kui Goldbach'i hüpotees kehtib, siis võib sellest lihtsasti teha järgmise järelduse:

Hüpotees 4 (Nõrk Goldbach'i hüpotees)

*Iga paaritu naturaalarv $n > 7$ on esitatav summana $n = a + b + c$, kus a , b ja c on (paaritud) **algarvud**.*

Mitmed matemaatikud on tõestanud, et nõrk Goldbach'i hüpotees kehtib kõigi piisavalt suurte arvude korral ("piisavalt suur" vähenes järjest kuni arvuni $\lfloor e^{3100} \rfloor \approx 2 \cdot 10^{1346}$). Lõpuks aastal 2013. tõestas peru matemaatik Harald Helfgott, et **nõrk Goldbach'i hüpotees kehtib** tõepoolest kõigi paaritute arvude korral.

Kui Goldbachi hüpotees kehtib, siis võib sellest lihtsasti teha järgmise järelduse:

Hüpotees 4 (Nõrk Goldbachi hüpotees)

*Iga paaritu naturaalarv $n > 7$ on esitatav summana $n = a + b + c$, kus a , b ja c on (paaritud) **algarvud**.*

Mitmed matemaatikud on tõestanud, et nõrk Goldbachi hüpotees kehtib kõigi piisavalt suurte arvude korral (“piisavalt suur” vähenes järjest kuni arvuni $\lfloor e^{3100} \rfloor \approx 2 \cdot 10^{1346}$). Lõpuks aastal 2013. tõestas peru matemaatik Harald Helfgott, et **nõrk Goldbachi hüpotees kehtib** tõepoolest kõigi paaritute arvude korral.

Kui Goldbach'i hüpotees kehtib, siis võib sellest lihtsasti teha järgmise järelduse:

Hüpotees 4 (Nõrk Goldbach'i hüpotees)

*Iga paaritu naturaalarv $n > 7$ on esitatav summana $n = a + b + c$, kus a , b ja c on (paaritud) **algarvud**.*

Mitmed matemaatikud on tõestanud, et nõrk Goldbach'i hüpotees kehtib kõigi piisavalt suurte arvude korral ("piisavalt suur" vähenes järjest kuni arvuni $\lfloor e^{3100} \rfloor \approx 2 \cdot 10^{1346}$). Lõpuks aastal 2013. tõestas peru matemaatik Harald Helfgott, et **nõrk Goldbach'i hüpotees kehtib** tõepoolest kõigi paaritute arvude korral.

Võib-olla üldse kuulsamaid **lahendatud** arvuteooria arvuteooria probleeme on aga järgmine.

Võrrandil $x + y = z$ on ilmselt väga palju **täisarvulisi** lahendeid.

Võrrandi $x^2 + y^2 = z^2$ täisarvulisi lahendeid on juba raskem leida, aga neid on samuti lõpmata palju. Viimaseid kutsutakse **Pythagorase kolmikuteks**, näiteks

$$3^2 + 4^2 = 5^2 \quad \text{ja} \quad 5^2 + 12^2 = 13^2.$$

Võrrandil $x^3 + y^3 = z^3$ on aga võrdlemisi vähe lahendeid. Need nimelt esinevad ainult kujudel $x = y, z = 0$; $x = z, y = 0$ või $y = z, x = 0$.

Võib-olla üldse kuulsamaid **lahendatud** arvuteooria arvuteooria probleeme on aga järgmine.

Võrrandil $x + y = z$ on ilmselt väga palju **täisarvulisi** lahendeid.

Võrrandi $x^2 + y^2 = z^2$ täisarvulisi lahendeid on juba raskem leida, aga neid on samuti lõpmata palju. Viimaseid kutsutakse **Pythagorase kolmikuteks**, näiteks

$$3^2 + 4^2 = 5^2 \quad \text{ja} \quad 5^2 + 12^2 = 13^2.$$

Võrrandil $x^3 + y^3 = z^3$ on aga võrdlemisi vähe lahendeid. Need nimelt esinevad ainult kujudel $x = y, z = 0$; $x = z, y = 0$ või $y = z, x = 0$.

Võib-olla üldse kuulsamaid lahendatud arvuteooria arvuteooria probleeme on aga järgmine.

Võrrandil $x + y = z$ on ilmselt väga palju täisarvulisi lahendeid.

Võrrandi $x^2 + y^2 = z^2$ täisarvulisi lahendeid on juba raskem leida, aga neid on samuti lõpmata palju. Viimaseid kutsutakse Pythagorase kolmikuteks, näiteks

$$3^2 + 4^2 = 5^2 \quad \text{ja} \quad 5^2 + 12^2 = 13^2.$$

Võrrandil $x^3 + y^3 = z^3$ on aga võrdlemisi vähe lahendeid. Need nimelt esinevad ainult kujudel $x = y, z = 0$; $x = z, y = 0$ või $y = z, x = 0$.

Võib-olla üldse kuulsamaid lahendatud arvuteooria arvuteooria probleeme on aga järgmine.

Võrrandil $x + y = z$ on ilmselt väga palju täisarvulisi lahendeid.

Võrrandi $x^2 + y^2 = z^2$ täisarvulisi lahendeid on juba raskem leida, aga neid on samuti lõpmata palju. Viimaseid kutsutakse Pythagorase kolmikuteks, näiteks

$$3^2 + 4^2 = 5^2 \quad \text{ja} \quad 5^2 + 12^2 = 13^2.$$

Võrrandil $x^3 + y^3 = z^3$ on aga võrdlemisi vähe lahendeid. Need nimelt esinevad ainult kujudel $x = y, z = 0$; $x = z, y = 0$ või $y = z, x = 0$.

Hüpoteesi, et selle ja veel kõrgema astme võrrandite $x^n + y^n = z^n$ lahendid ongi vaid sellisel kujul, püstitas 1637. aastal prantsuse matemaatik Pierre de Fermat.

Hüpotees 5 (Fermat' suur teoreem)

Kui $n \geq 3$ on naturaalarv, siis võrrandil

$$x^n + y^n = z^n$$

ei ole selliseid ratsionaalarvulisi lahendeid, kus vähemalt ühe muutuja väärtus ei ole 0.

Hüpoteesi, et selle ja veel kõrgema astme võrrandite $x^n + y^n = z^n$ lahendid ongi vaid sellisel kujul, püstitas 1637. aastal prantsuse matemaatik Pierre de Fermat.

Hüpotees 5 (Fermat' suur teoreem)

Kui $n \geq 3$ on naturaalarv, siis võrrandil

$$x^n + y^n = z^n$$

ei ole selliseid ratsionaalarvulisi lahendeid, kus vähemalt ühe muutuja väärtus ei ole 0.

Järgmise rohkem kui 300 aasta jooksul näidati, et see hüpotees kehtib järjest **suuremate** astendajate n korral ja isegi tervete naturaalarvude **klasside** jaoks, aga üldjuht jäi püüdmatuks kuni möödunud sajandi üheksakümnenadeni.

Inglise matemaatik **Andrew Wiles** töötas aastatel 1986-1993 suhtelises salajasuses selle teoreemi tõestamiseks vajalike diofantilise geomeetria tulemuste kallal ja kuulutas kõigi üllatuseks **1993.** aasta suvel, et on tõestanud rea tulemusi, millest muuseas järeldeb Fermat' suur teoreem.

Kahjuks oli tema mõttekäigus oluline lünk ja ta püüdis 1994. aasta sügiseni seda parandada, alguses üksi ja siis koos teise inglise matemaatiku Richard Tayloriga.

Septembris 1994. tuli ta lõpuks ideele, mis lünga täitis ja 1995. aasta maikuus, **358 aastat** peale probleemi püstitamist, nägid tema tulemused lõplikult kontrollituna ajakirjas *Annals of Mathematics* trükivalgust.

Järgmise rohkem kui 300 aasta jooksul näidati, et see hüpotees kehtib järjest **suuremate** astendajate n korral ja isegi tervete naturaalarvude **klasside** jaoks, aga üldjuht jäi püüdmatuks kuni möödunud sajandi üheksakümnenadeni.

Inglise matemaatik **Andrew Wiles** töötas aastatel 1986-1993 suhtelises salajasuses selle teoreemi tõestamiseks vajalike diofantilise geomeetria tulemuste kallal ja kuulutas kõigi üllatuseks **1993.** aasta suvel, et on tõestanud rea tulemusi, millest muuseas järeldeb Fermat' suur teoreem.

Kahjuks oli tema mõttekäigus oluline lünk ja ta püüdis 1994. aasta sügiseni seda parandada, alguses üksi ja siis koos teise inglise matemaatiku Richard Tayloriga.

Septembris 1994. tuli ta lõpuks ideele, mis lünga täitis ja 1995. aasta maikuus, **358 aastat** peale probleemi püstitamist, nägid tema tulemused lõplikult kontrollituna ajakirjas *Annals of Mathematics* trükivalgust.

Järgmise rohkem kui 300 aasta jooksul näidati, et see hüpotees kehtib järjest **suuremate** astendajate n korral ja isegi tervete naturaalarvude **klasside** jaoks, aga üldjuht jäi püüdmatuks kuni möödunud sajandi üheksakümnenadeni.

Inglise matemaatik **Andrew Wiles** töötas aastatel 1986-1993 suhtelises salajasuses selle teoreemi tõestamiseks vajalike diofantilise geomeetria tulemuste kallal ja kuulutas kõigi üllatuseks **1993.** aasta suvel, et on tõestanud rea tulemusi, millest muuseas järeldeb Fermat' suur teoreem.

Kahjuks oli tema mõttekäigus oluline lünk ja ta püüdis 1994. aasta sügiseni seda parandada, alguses üksi ja siis koos teise inglise matemaatiku Richard Tayloriga.

Septembris 1994. tuli ta lõpuks ideele, mis lünga täitis ja 1995. aasta maikuus, **358 aastat** peale probleemi püstitamist, nägid tema tulemused lõplikult kontrollituna ajakirjas *Annals of Mathematics* trükivalgust.

Järgmise rohkem kui 300 aasta jooksul näidati, et see hüpotees kehtib järjest **suuremate** astendajate n korral ja isegi tervete naturaalarvude **klasside** jaoks, aga üldjuht jäi püüdmatuks kuni möödunud sajandi üheksakümnendateni.

Inglise matemaatik **Andrew Wiles** töötas aastatel 1986-1993 suhtelises salajasuses selle teoreemi tõestamiseks vajalike diofantilise geomeetria tulemuste kallal ja kuulutas kõigi üllatuseks **1993.** aasta suvel, et on tõestanud rea tulemusi, millest muuseas järeldeb Fermat' suur teoreem.

Kahjuks oli tema mõttekäigus oluline lünk ja ta püüdis 1994. aasta sügiseni seda parandada, alguses üksi ja siis koos teise inglise matemaatiku Richard Tayloriga.

Septembris 1994. tuli ta lõpuks ideele, mis lünga täitis ja 1995. aasta maikuus, **358 aastat** peale probleemi püstitamist, nägid tema tulemused lõplikult kontrollituna ajakirjas *Annals of Mathematics* trükivalgust.

Loodetavasti ei ole teil praegu selline tunne...

