

Arvuteooria

Diskreetse matemaatika elemendid

Sügis 2008

Olgu a ja b täisarvud.

- ▶ Kui leidub selline täisarv m , et $b = am$, siis ütleme, et arv a **jagab** arvu b ehk arv b **jagub** arvuga a .

Tähistused:

- ▶ $a \mid b$ arv a jagab arvu b
- ▶ $b : a$ arv b jagub arvuga a

Näiteks

$$3 \mid 111 \quad 7 \mid -91 \quad -7 \mid -91$$

Tegurid

Kui $a \mid b$, siis

- ▶ arvu a nimetatakse arvu b **teguriks** ehk **jagajaks**
- ▶ arvu b nimetatakse arvu a **kordseks**

Jaguvuse definitsiooni põhjal on arv a arvu b tegur, kui leidub selline täisarv m , et $b = am$.

- ▶ Igal täisarvul b on vähemalt järgmised tegurid: 1 , -1 , b , $-b$.
- ▶ Iga täisarvu a korral $a \mid 0$, vastupidine seos $0 \mid a$ kehtib parajasti siis, kui $a = 0$. Seega $0 \mid 0$.
- ▶ Iga täisarvu b korral $1 \mid b$, vastupidine $b \mid 1$ kehtib parajasti siis, kui $b = 1$ või $b = -1$.

Jaguvuse lihtsamad omadused

Täisarvude hulgal määratud jaguvusrelatsioonil on järgmised omadused.

- ▶ **Refleksiivus:** iga täisarvu a korral $a \mid a$.
- ▶ Kui $a \mid b$ ja $b \mid a$, siis $a = b$ või $a = -b$.
- ▶ **Transitiivsus:** kui $a \mid b$ ja $b \mid c$, siis $a \mid c$.

Tõestamiseks kasutada jaguvuse definitsiooni.

Jaguvuse seos tehetega

- ▶ Kui $a \mid b$, siis $\pm a \mid \pm b$.
- ▶ Kui $a \mid b$ ja $a \mid c$, siis suvaliste täisarvude s ja t korral $a \mid bs + ct$.
- ▶ $a \mid b$ parajasti siis, kui iga täisarvu c korral $ac \mid bc$.

Esimene omadus tähendab, et jaguvuse uurimisel võime piirduda mittenegatiivsete täisarvudega.

Teisest omadusest järeldub, et kui arv a jagab arve b ja c , siis jagab ta ka nende arvude summat ja vahet.

Jäägiga jagamine

Olgu a ja b täisarvud, kusjuures $a > 0$.

Jäägiga jagamine tähendab arvu b esitamist kujul

$$b = aq + r, \quad \text{kus } 0 \leq r < a.$$

Siin on

b jagatav

a jagaja

q jagatis

r jääk

Näiteks kui $a = 3$ ja $b = 17$, siis

$$17 = 3 \cdot 5 + 2.$$

Negatiivsete arvude jagamine

Näiteks kui $b = -17$ ja $a = 3$, siis

$$-17 = 3 \cdot (-6) + 1$$

Jääk on alati **mittenegatiivne**.

Võrduses $b = a \cdot q + r$ **peab alati** kehtima $0 \leq r < a$.

Arvu b saab alati nii esitada, sest jadas

$$\dots, -3a, -2a, -a, 0, a, 2a, 3a, \dots$$

saab alati leida kaks järjestikust arvu, mille vahel b asub.

Algarv ja kordarv

Vaatleme järgnevalt ainult positiivseid täisarve ja nende positiivseid tegureid.

Igal positiivsel täisarvul a on kindlasti olemas tegurid 1 ja a .

- ▶ **Algarv** on selline ühest suurem naturaalarv n , millel pole rohkem positiivseid tegureid kui 1 ja n .
- ▶ **Kordarv** on selline ühest suurem naturaalarv n , millel on ka muid positiivseid tegureid peale 1 ja n .
- ▶ Arv 1 ei ole ei algarv ega kordarv.

Algarvud: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, ...

Kordarvud: 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, ...

Kuidas teha kindlaks, kas etteantud naturaalarv n on algarv?

- ▶ Kontrollida läbi kõik arvud $2, \dots, n - 1$. Kui n ei jagu ühegi nendest, siis ta on algarv.
- ▶ Kontrollida läbi kõik arvud $2, \dots, \sqrt{n}$. Kui n on kordarv, siis tal leidub tegur ka nende arvude hulgas.
- ▶ Tõenäosuslikud polünomiaalsed meetodid (Rabin-Milleri test).
- ▶ Polünomiaalne algoritm (2002).

Teoreem

(Eukleides.) Leidub lõpmata palju algarve.

Tõestus. Oletame, et algarve on lõplik hulk:

$$p_1, \quad p_2, \quad p_3, \quad \dots, \quad p_k.$$

Vaatleme arvu

$$n = p_1 p_2 p_3 \dots p_k + 1$$

See ei jagu algarvudega $p_1, p_2, \dots, p_k$, sest ta annab nendega jagades jäägi 1. Järelikult on n ise algarv või tal leidub algarvuline tegur, mis erineb algarvudest $p_1, p_2, \dots, p_n$, kummalgi juhul vastuolu.

Tõestus 2. Tõestame, et iga naturaalarvu n jaoks leidub temast suurem algarv.

Olgu p arvu $n! + 1$ vähim ühest erinev tegur. Siis

- ▶ p on algarv, sest kui tal leiduks tegur 1 ja p vahel, siis see tegur oleks ka arvu $n! + 1$ tegur.
- ▶ $p > n$, sest $n! + 1$ ei jagu ühegi arvuga $2, 3, \dots, n$.

- ▶ Kirjutame välja kõik arvud $1, 2, \dots, n$.
- ▶ Kriipsutame maha arvu 1.
- ▶ Järgmine allesjääv arv on 2; kriipsutame maha kõik arvu 2 kordsed.
- ▶ Järgmine allesjääv arv on 3; kriipsutame maha kõik arvu 3 kordsed.
- ▶ Järgmine allesjääv arv on 5 jne.
- ▶ Algarvud on parajasti need, mis protsessi lõppedes alles jäävad.

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

×	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

×	2	3	×	5	×	7	×	9	×
11	×	13	×	15	×	17	×	19	×
21	×	23	×	25	×	27	×	29	×
31	×	33	×	35	×	37	×	39	×
41	×	43	×	45	×	47	×	49	×
51	×	53	×	55	×	57	×	59	×
61	×	63	×	65	×	67	×	69	×
71	×	73	×	75	×	77	×	79	×
81	×	83	×	85	×	87	×	89	×
91	×	93	×	95	×	97	×	99	×

×	2	3	×	5	×	7	×	×	×
11	×	13	×	×	×	17	×	19	×
×	×	23	×	25	×	×	×	29	×
31	×	×	×	35	×	37	×	×	×
41	×	43	×	×	×	47	×	49	×
×	×	53	×	55	×	×	×	59	×
61	×	×	×	65	×	67	×	×	×
71	×	73	×	×	×	77	×	79	×
×	×	83	×	85	×	×	×	89	×
91	×	×	×	95	×	97	×	×	×

×	2	3	×	5	×	7	×	×	×
11	×	13	×	×	×	17	×	19	×
×	×	23	×	25	×	×	×	29	×
31	×	×	×	35	×	37	×	×	×
41	×	43	×	×	×	47	×	×	×
×	×	53	×	55	×	×	×	59	×
61	×	×	×	65	×	67	×	×	×
71	×	73	×	×	×	×	×	79	×
×	×	83	×	85	×	×	×	89	×
×	×	×	×	95	×	97	×	×	×

Algarvude jaotumine

- ▶ Algarvud paiknevad naturaalarvude jadas väga ebaühtlaselt.
- ▶ Kaks algarvu võivad asuda järjest. Ainukesed sellised on 2 ja 3.
- ▶ Kui kaks algarvu erinevad teineteisest kahe võrra, siis nimetatakse neid **kaksikalgarvudeks**. Näiteks 3557 ja 3559. On oletus, et kaksikute paare on lõpmata palju.
- ▶ Leidub kui tahes pikki lõike, milles pole ühtegi algarvu, näiteks $n! + 2$, $n! + 3$, $\dots$, $n! + n$ on järjestikused kordarvud.
- ▶ Jaotusdiagramm:



- ▶ Algarvude jaotumist kirjeldab algarvufunktsioon

$$\pi(n) = \text{algarvude arv hulgas } \{1, 2, \dots, n\}$$

- ▶ Esimesed väärtused:

$$\begin{array}{cccc} \pi(1) = 0 & \pi(2) = 1 & \pi(3) = 2 & \pi(4) = 2 \\ \pi(5) = 3 & \pi(6) = 3 & \pi(7) = 4 & \pi(8) = 4 \end{array}$$

Teoreem

Kehtib asümptootiline ekvivalents

$$\pi(n) \approx \frac{n}{\ln n}$$

Valemi tuletas C. F. Gauss 18. sajandi lõpul algarvude tabeli analüüsimisel.

Tõestasid J. Hadamard ja C. de la Vallée Poussin teineteisest sõltumatult aastal 1896.

On olemas ka täpsemaid empiirilisi valemeid, näiteks

$$\pi(n) \approx \frac{n}{\ln n - 1,08366} \quad (\text{Legendre}) \quad \pi(n) \approx \int_2^n \frac{dt}{\ln t} \quad (\text{Gauss})$$

Leida, kui suur on 200-kohaliste arvude hulgas algarvude osakaal.

- ▶ 200-kohalisi arve on

$$10^{200} - 10^{199} = 9 \cdot 10^{199}$$

- ▶ 200-kohalisi algarve on ligikaudu

$$\pi(10^{200}) - \pi(10^{199}) \approx \frac{10^{200}}{\ln 10^{200}} - \frac{10^{199}}{\ln 10^{199}} \approx 1,95 \cdot 10^{197}$$

- ▶ Algarvude osakaal on ligikaudu

$$\frac{1,95 \cdot 10^{197}}{9 \cdot 10^{199}} \approx \frac{1}{460}$$

Arvu lahutamine algtegurite korrutiseks

- ▶ Kui arv ei ole algarv, siis saab ta esitada kahe väiksema teguri korrutisena.
- ▶ Kui mõni saadud teguritest ei ole algarv, siis saab selle teguri esitada kahe väiksema teguri korrutisena jne.
- ▶ Järelikult saab iga arvu, mis pole algarv, esitada algarvude korrutisena.
- ▶ Kui arv juba on algarv, siis tõlgendame teda korrutisena, kus esineb ainult üks tegur.

Teoreem

Iga ühest suurema naturaalarvu saab parajasti ühel viisil esitada algarvude korrutisena, arvestamata tegurite järjekorda.

Tõestuse skeem. Oletame, et leidub naturaalarve, millel on kaks esitust algarvude korrutisena. Olgu n **vähim** selline naturaalarv.

Tõestame, et siis saab leida naturaalarvu n' , mis on väiksem kui n ja millel on samuti kaks esitust algarvude korrutisena.

Et n juba oli vähim selline arv, siis tähendab see vastuolu.

- ▶ Iga naturaalarvu n saab esitada kujul

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

- ▶ Siin on $p_1, p_2, \dots, p_k$ kõik algarvud, millega n jagub, ning $\alpha_1, \alpha_2, \dots, \alpha_k$ nende algarvude kordsused.
- ▶ Aritmeetika põhiteoreemist järeldeb, et see esitus on ühene.
- ▶ Seda esitust nimetatakse naturaalarvu n **kanooniliseks kujuks**.
- ▶ Näiteks: $600 = 2^3 \cdot 3 \cdot 5$, $35 = 5 \cdot 7$,
 $5\,251\,400 = 2^3 \cdot 5^2 \cdot 7 \cdot 11^2 \cdot 31$

Teoreem

Olgu n naturaalarv kanoonilise kujuga

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

Naturaalarv m on arvu n tegur parajasti siis, kui m avaldub kujul

$$m = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$$

kus iga $i = 1, 2, \dots, k$ korral $0 \leq \beta_i \leq \alpha_i$.

Arvu tegurite arv

- ▶ Arvu kanoonilise kuju põhjal saab leida arvu tegurite arvu ilma neid välja kirjutamata.

- ▶ Kui

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

siis arvu n teguris peab algteguri p_1 astendaja olema üks arvudest $0, \dots, \alpha_1$, algteguri p_2 astendaja üks arvudest $0, \dots, \alpha_2$ jne.

- ▶ Tegurite arv on seega

$$(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$$

- ▶ Näiteks arvul $694\,575 = 3^4 \cdot 5^2 \cdot 7^3$ on $(4 + 1)(2 + 1)(3 + 1) = 60$ tegurit.

Fermat' väike teoreem

Teoreem

Kui p on algarv, siis iga täisarvu a korral, mis ei jagu p -ga, kehtib seos $p \mid a^{p-1} - 1$.

Tõestuse skeem. Vaatleme arve

$$1, 2, \dots, p-1$$

Korrutades neid a -ga, saame

$$a, 2a, \dots, (p-1)a$$

Tõestame, et need arvud annavad p -ga jagades parajasti jäägid $1, 2, \dots, p-1$ mingis järjekorras. Järelikult annavad arvud

$$a \cdot 2a \cdot \dots \cdot (p-1)a \quad \text{ja} \quad 1 \cdot 2 \cdot \dots \cdot (p-1)$$

jagamisel p -ga sama jäägi ning nende vahe $(p-1)!(a^p - 1)$ jagub p -ga. Et $(p-1)!$ ei jagu algarvuga p , siis peab $a^p - 1$ jaguma p -ga.

Järeldus

Kui p on algarv, siis iga täisarvu a korral $p \mid a^p - a$.

Tõestus.

- ▶ Kui a ei jagu p -ga, siis teoreemi põhjal $p \mid a^{p-1} - 1$ ja seega $p \mid (a^{p-1} - 1)a$.
- ▶ Kui a jagub p -ga, siis a^p ja a annavad p -ga jagamisel mõlemad jäägi 0.

- ▶ Fermat' teoreemi väide võib mõnikord kehtida ka siis, kui p ei ole algarv.
- ▶ Näiteks olgu $p = 341 = 11 \cdot 31$ ning $a = 2$.

$$2^{340} = (2^{10})^{34} = 1024^{34}$$

annab 341-ga jagamisel jäägi 1, sest 1024 annab jäägi 1.

- ▶ Arv 341 on **pseudoalgarv** alusel 2.
- ▶ Siiski, 341 ei rahulda Fermat' teoreemi väidet, kui aluseks võtta mingi muu arv, nt 3^{340} annab 341-ga jagades jäägi 56.

- ▶ Paaritu kordarv, mis rahuldab Fermat' teoreemi väidet iga aluse korral, mis on selle kordarvuga ühistegurita (st on pseudoalgarv kõigil neil alustel).
- ▶ Näiteks olgu $p = 561 = 3 \cdot 11 \cdot 17$ ning $SÜT(a, p) = 1$. Siis

$$a^{560} = (a^2)^{280} \text{ annab 3-ga jagamisel jäägi 1}$$

$$a^{560} = (a^{10})^{56} \text{ annab 11-ga jagamisel jäägi 1}$$

$$a^{560} = (a^{16})^{35} \text{ annab 17-ga jagamisel jäägi 1}$$

Seega $a^{560} - 1$ jagub nii 3-ga, 11-ga kui 17-ga.

- ▶ <http://www.research.att.com/~njas/sequences>, jada number A002997

- ▶ Naturaalarvude a ja b **ühisteguriks** nimetatakse iga naturaalarvu, millega jagub nii a kui ka b .
 - ▶ Näiteks arvude 36 ja 60 ühistegurid on 1, 2, 3, 4, 6, 12.
- ▶ Naturaalarvude a ja b **suurimaks ühisteguriks** nimetatakse nende ühistegurite hulgast suurimat.
 - ▶ Näiteks arvude 36 ja 60 suurim ühistegur on 12.
- ▶ Suurim ühistegur on alati olemas, sest iga kahe arvu ühistegurite hulk on mittetühi.
- ▶ Analoogiliselt defineeritakse mitme arvu $a_1, a_2, \dots, a_n$ ühistegur ja nende arvude suurim ühistegur.

- ▶ Arvude a ja b suurimat ühistegurit tähistatakse:

$$\text{SÜT}(a, b) = \text{gcd}(a, b) \quad (a, b)$$

- ▶ Seega:

$$\text{SÜT}(36, 60) = 12 \quad \text{SÜT}(8, 1) = 1$$

- ▶ Mõnikord defineeritakse veel $\text{SÜT}(a, 0) = a$ iga a korral. Siis näiteks

$$\text{SÜT}(3, 0) = 3 \quad \text{SÜT}(0, 0) = 0$$

Ühistegurita arvud

- ▶ Naturaalarve, mille suurim ühistegur on 1, nimetatakse **ühistegurita arvudeks**.
 - ▶ Näiteks 16 ja 25 on ühistegurita, 99 ja 100 on ühistegurita jne.
- ▶ Jagades naturaalarvud a ja b nende suurima ühisteguriga d , jäävad järele ühistegurita arvud:

$$\text{SÜT} \left(\frac{a}{d}, \frac{b}{c} \right) = 1$$

- ▶ Iga kaks naturaalarvu a ja b saab esitada kujul $a = a'd$ ja $b = b'd$, kus d on arvude a ja b suurim ühistegur ning a' ja b' on ühistegurita.

Ühistegur kanoonilise kuju järgi

Kui

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

ja

$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$$

siis

$$\text{SÜT}(a, b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \dots p_k^{\min(\alpha_k, \beta_k)}$$

Ühisteguri teine definitsioon

- ▶ Kanoonilisest kujust järeldub, et arvude a ja b suurim ühistegur jagub arvude a ja b iga ühisteguriga.
- ▶ Antud arvude suurimat ühistegurit võib defineerida ka kui arvu, mis jagub nende arvude iga ühisteguriga.
- ▶ See võimaldab ühisteguri mõistet laiendada ka sellistele hulkadele, kus on määratud jaguvus, aga mitte järjestus (nt polünoomid, Gaussi täisarvud jne).
- ▶ Keerulisemaks muutub suurima ühisteguri olemasolu tõestamine: kõigi ühisteguritega jaguva ühisteguri leidumine pole sellise definitsiooni korral nii vahetult selge.

Suurima ühisteguri homogeensus

Teoreem

Iga naturaalarvu n korral

$$S\ddot{U}T(na, nb) = n S\ddot{U}T(a, b)$$

Tõestuse skeem. Olgu $d = S\ddot{U}T(a, b)$. Tõestame, et

1. nd on arvude na ja nb ühistegur
2. nd on arvude na ja nb ühistegurite hulgas suurim

Suurima ühisteguri homogeensus

Järeldus

Kui c on arvude a ja b ühistegur, siis

$$\text{SÜT}\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{\text{SÜT}(a, b)}{c}$$

Tõestus.

$$c \text{SÜT}\left(\frac{a}{c}, \frac{b}{c}\right) = \text{SÜT}(a, b)$$

Ühistegurita arvude omadused

Teoreem

Kui $SÜT(a, b) = 1$, siis iga naturaalarvu c korral

$$SÜT(ac, b) = SÜT(c, b).$$

Tõestuse skeem. Tõestame, et

1. arvu $SÜT(ac, b)$ iga tegur on ka arvu $SÜT(c, b)$ tegur
2. arvu $SÜT(c, b)$ iga tegur on ka arvu $SÜT(ac, b)$ tegur

Järelikult ühtib arvude ac ja b ühistegurite hulk arvude c ja b ühistegurite hulgaga.

- ▶ Kui $S\ddot{U}T(a, c) = 1$ ja $S\ddot{U}T(b, c) = 1$, siis $S\ddot{U}T(ab, c) = 1$
- ▶ Kui $a \mid bc$ ja $S\ddot{U}T(a, b) = 1$, siis $a \mid c$.
- ▶ Kui $a \mid c$ ja $b \mid c$ ning $S\ddot{U}T(a, b) = 1$, siis $ab \mid c$.

Leida $\text{SÜT}(560, 315)$.

$$\begin{aligned}\text{SÜT}(560, 315) &= \text{SÜT}(5 \cdot 112, 5 \cdot 63) \\ &= 5 \text{SÜT}(112, 63) \\ &= 5 \text{SÜT}(2^4 \cdot 7, 63) \\ &= 5 \text{SÜT}(7, 63) \\ &= 5 \cdot 7 \\ &= 35\end{aligned}$$

Mitme arvu suurim ühistegur

Teoreem

Arvude $a_1, a_2, \dots, a_n$ suurim ühistegur on

$$\text{SÜT}(a_1, a_2, \dots, a_n) = \text{SÜT}(\dots \text{SÜT}(\text{SÜT}(a_1, a_2), a_3), \dots, a_n)$$

Tõestus. Kui $n = 2$, siis väide kehtib.

Kui $n = k + 1$, siis tuleb tõestada võrdus

$$\text{SÜT}(a_1, a_2, \dots, a_k, a_{k+1}) = \text{SÜT}(\text{SÜT}(a_1, a_2, \dots, a_k), a_{k+1})$$

See järeldeb asjaolust, et suvalise d korral on seosed

$$d \mid a_1, \quad d \mid a_2, \quad \dots, \quad d \mid a_k, \quad d \mid a_{k+1}$$

samaväärsed seostega

$$d \mid \text{SÜT}(a_1, a_2, \dots, a_k), \quad d \mid a_{k+1}$$

Algoritm kahe arvu suurima ühisteguri arvutamiseks.

Olgu a ja b mittenegatiivsed täisarvud.

- ▶ Kui $b = 0$, siis lõpetada töö.
- ▶ Leida a jagamisel b -ga tekkiv jääk r . Võtta a uueks väärtuseks b senine väärtus ja b uueks väärtuseks r .
- ▶ Minna tagasi esimesele sammule.

Tulemuseks on a väärtus.

Olgu $a = 2322$, $b = 654$.

2322 654

Olgu $a = 2322$, $b = 654$.

2322	654
------	-----

Olgu $a = 2322$, $b = 654$.

2322 654 360

Olgu $a = 2322$, $b = 654$.

2322	654	360
------	-----	-----

Olgu $a = 2322$, $b = 654$.

2322 654 360 294

Olgu $a = 2322$, $b = 654$.

2322	654	360	294
------	-----	-----	-----

Olgu $a = 2322$, $b = 654$.

2322 654 360 294 66

Olgu $a = 2322$, $b = 654$.

2322	654	360	294	66
------	-----	-----	-----	----

Olgu $a = 2322$, $b = 654$.

2322 654 360 294 66 30

Olgu $a = 2322$, $b = 654$.

2322	654	360	294	66	30
------	-----	-----	-----	----	----

Olgu $a = 2322$, $b = 654$.

2322 654 360 294 66 30 6

Olgu $a = 2322$, $b = 654$.

2322

654

360

294

66

30

6

Olgu $a = 2322$, $b = 654$.

2322	654	360	294	66	30	6	0
------	-----	-----	-----	----	----	---	---

Olgu $a = 2322$, $b = 654$.

2322	654	360	294	66	30	6	0
------	-----	-----	-----	----	----	---	---

$\text{SÜT}(2322, 654) = 6$

- ▶ Kas algoritm lõpetab alati töö?
- ▶ Kas algoritm annab alati vastuseks suurima ühisteguri?
- ▶ Milline on algoritmi efektiivsus?

Eukleidese algoritmi peatumine

- ▶ Igal sammul asendatakse arvupaar (a, b) paariga (b, r) , kus r on a jagamisel b -ga tekkiv jääk.
- ▶ Järelikult $r < b$.
- ▶ Samme korrates väheneb vaadeldava arvupaari teine komponent ning saab varem või hiljem nulliks.

Teoreem

Kui r on jääk, mis tekib arvu a jagamisel arvuga b , siis
 $SÜT(a, b) = SÜT(b, r)$.

Tõestus. Võrdusest $a = bq + r$ näeme, et

1. kui $d \mid a$ ja $d \mid b$, siis $d \mid r$
2. kui $d \mid b$ ja $d \mid r$, siis $d \mid a$

Järelikult on arvude a ja b ühistegurite hulk sama mis arvude b ja r ühistegurite hulk.

Viimasel sammul saame arvud r ja 0 , nende suurim ühistegur on r .

Teoreem

Arvude a ja b (kus $a > b$) suurima ühisteguri leidmiseks kulub Eukleidese algoritmi puhul ülimalt

$$1 + \log_2 a + \log_2 b$$

sammu.

Tõestus. Ühe sammuga asendatakse arvupaar (a, b) paariga (b, r) . Seejuures $br < ab/2$ ehk ühel sammul väheneb arvude korrutis vähemalt 2 korda.

Kui pärast k sammu on korrutis veel positiivne, siis peab kehtima $ab/2^k \geq 1$, millest

$$k \leq \log_2(ab) = \log_2 a + \log_2 b$$

Algoritmi töö algebralisel kujul

$$a = bq_1 + r_1$$

r_1 avaldub b ja a kaudu

$$b = r_1q_2 + r_2$$

r_2 avaldub r_1 ja b kaudu

$$r_1 = r_2q_3 + r_3$$

r_3 avaldub r_2 ja r_1 kaudu

.....

.....

$$r_{k-3} = r_{k-2}q_{k-1} + r_{k-2}$$

r_{k-1} avaldub r_{k-2} ja r_{k-3} kaudu

$$r_{k-2} = r_{k-1}q_k + r_k$$

r_k avaldub r_{k-1} ja r_{k-2} kaudu

$$r_{k-1} = r_kq_{k+1}$$

Avaldame eelviimasest seosest r_k ja asendame saadud avaldises järk-järgult r_{k-1} , r_{k-2} , ... eelnevate seoste põhjal.

Järelikult r_k avaldub a ja b lineaarkombinatsioonina.

Naturaalarvude a ja b suurima ühisteguri võib avaldada kujul

$$\text{SÜT}(a, b) = as + bt$$

kus s ja t on täisarvud.

Näiteks olgu $a = 360$ ja $b = 294$.

$$360 = 294 \cdot 1 + 66$$

$$294 = 66 \cdot 4 + 30$$

$$66 = 30 \cdot 2 + 6$$

$$30 = 6 \cdot 5$$

$$6 = 66 - 30 \cdot 2$$

$$6 = 66 - (294 - 66 \cdot 4) \cdot 2 =$$

$$= 294 \cdot (-2) + 66 \cdot 9$$

$$6 = 294 \cdot (-2) + (360 - 294 \cdot 1) \cdot 9 =$$

$$= 294 \cdot (-11) + 360 \cdot 9$$

- ▶ Lineaarne diofantiline võrrand:

$$ax + by = c$$

kus a , b ja c on antud täisarvud, vaja leida täisarvud x ja y .

- ▶ Kui $\text{SÜT}(a, b) \mid c$, siis saame leida arvud x_0 ja y_0 nii, et

$$ax_0 + by_0 = \text{SÜT}(a, b)$$

ning korrutada tulemust arvuga $\frac{c}{\text{SÜT}(a, b)}$.

- ▶ Kui $\text{SÜT}(a, b) \nmid c$, siis võrrandil lahendeid ei leidu.

- ▶ Naturaalarvude a ja b **ühiskordseks** nimetatakse iga naturaalarvu, mis jagub nii a -ga kui ka b -ga.
- ▶ Naturaalarvude a ja b **vähimaks ühiskordseks** nimetatakse nende ühiskordsete hulgast vähimat.
- ▶ Tähised:

$$\text{VÜK}(a, b) \quad \text{lcm}(a, b) \quad [a, b]$$

- ▶ Näiteks

$$\text{VÜK}(6, 4) = 12 \quad \text{VÜK}(8, 1) = 8 \quad \text{VÜK}(24, 25) = 600$$

Vähim ühiskordne kanoonilise kuju järgi

Kui

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

ja

$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$$

siis

$$\text{SÜT}(a, b) = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \dots p_k^{\max(\alpha_k, \beta_k)}$$

Teoreem

Kehtib võrdus

$$\text{VÜK}(a, b) \text{ SÜT}(a, b) = ab$$

Järeldus

Kui $\text{SÜT}(a, b) = 1$, siis $\text{VÜK}(a, b) = ab$.

- ▶ Selle seose tõttu kanduvad mitmed suurima ühisteguri omadused üle vähimale ühiskordsele.
- ▶ Näiteks saab ka vähima ühiskordse arvutamiseks kasutada Eukleidese algoritmi.

Vähima ühiskordse seos jaguvusega

Järeldus

Arvude a ja b vähim ühiskordne on nende arvude iga ühiskordse tegur.

Tõestus. Olgu k arvude a ja b mingi ühiskordne. Tõestame, et

$$\text{SÜT} \left(\frac{k}{a}, \frac{k}{b} \right) \text{VÜK}(a, b) = k$$

Tõepoolest, eelmise teoreemi põhjal

$$ab \text{SÜT} \left(\frac{k}{a}, \frac{k}{b} \right) \text{VÜK}(a, b) = k \text{SÜT}(b, a) \text{VÜK}(a, b) = kab$$

Vähima ühiskordse homogeensus

Teoreem

Iga naturaalarvu n korral

$$\text{VÜK}(na, nb) = n \text{VÜK}(a, b)$$

Järeldus

Kui c on arvude a ja b ühistegur, siis

$$\text{VÜK}\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{\text{VÜK}(a, b)}{c}$$

Samuti kanduvad vähimale ühiskordsele üle ka paljud muud suurima ühisteguri omadused (või nende analoogid).