RSA tööd selgitavad algebralised faktid

Sven Laur

22. aprill 2002

1 Rühma mõiste ja näited

Definitsioon 1. Rühmaks nimetatakse hulka G, millel on defineeritud kahekohaline funktsioon(tehe) $\bullet(\cdot,\cdot) : G \times G \to G$, mis rahuldab järgmisi tingimusi

$$\forall x, y, z \in G \quad (x \cdot y) \cdot z = x \cdot (y \cdot z) \tag{1}$$

$$\exists 1 \in G \, \forall x \in G \quad x \cdot 1 = 1 \cdot x = x \tag{2}$$

Lisaks sellele peavad iga $a, y \in G$ lahenduma võrrandid

$$ax = y \qquad za = y \tag{3}$$

see tähendab peavad leiduma elemendid $x, z \in G$ nii, et võrrandid (3) oleksid täidetud. Rühma tähistatakse harilikult $(G; \cdot)$.

Märkus. Ühikelement 1 on lihtsalt sellise elemendi tähis, mis rahuldab tingimust (2) ning ei ole kuidagi seotud arvuga 1. See tähis on kasutusele võetud vaid selle pärast, et arv 1 käitub korrutamise suhtes sama moodi nagu rühma ühikelement.

Näide 1. Tähistame paarisarvude hulga $2\mathbb{Z}$ ning vaatleme tavalist korrutamist. Kahe paarisarvu korrutis on paarisarv ning lihtne on veenduda, et suvaliste paarisarvude korral on täidetud omadus (1). Kuna 1 pole paarisarv ning ei leidu teist arvu e mille korral $xe = ex = x$, siis paarisarvude hulk pole korrutamise suhtes rühm.

Näide 2. Vaatame sõnesid(*stringe*) ning nendel defineeritud ühendamise operatsiooni ., mis toimib nii 'ema'.'isa'='emaisa'. Jällegi on lihtne veenduda, et kolme sõne ühendamisel pole vahet millises järjekorras me seda teeme, seni kuni me sõnede järjekorda ei vaheta. Seega on täidetud omadus (1). Teisalt tühja sõne 1 ='' korral saame ükskõik millise teise sõne x korral $1.x = x.1$, seega on täidetud ka omadus (2). Samas võrrand

$$\text{`i'}.x = \text{`ema'}$$

ei ole lahenduv, kuna meil pole võimalik kaotada sõna eest tähte 'i' ning seega pole sõned ühendamise suhtes rühm.

Näide 3. Vaatme kõiki ratsionaalarve $\mathbb{Q}$, siis on alati täidetud omadused (1) ja (2). Võrrandit $ax = y$ õnnestub alati lahendada, kui $a \neq 0$. Paneme tähele, et iga kahe nullist erineva ratsionaalarvu korrutis on ka nullist erinev ja 1 on nullist erinev. Seega kui me vaatleme vaid nullist erinevaid elemente $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, siis on ka võrrandid (3) alati lahenduvad ning seetõttu on $(\mathbb{Q}^*; \cdot)$ rühm. Veelgi enam hulk $E = \{1\}$ on kinnine korrutamise suhtes ja rahuldab tingimusi (1), (2) ja (3), mistõttu ka $(E; \cdot)$ on rühm, kusjuures $E \subseteq \mathbb{Q}^*$.

Erilisteks võrranditeks rühmas on $ax = 1$ ja $za = 1$. On võimalik tõestada, et rühma iga elemendi a korral on mõlemal võrrandil ühesugune lahend $x = z$. Seetõttu nimetatakse võrrandi $ax = xa = 1$ lahendit x elemendi a pöördelemendiks ning tähistatakse a^{-1}. Viimasest näitest lähtudes, saame defieerida alamrühma.

Definitsioon 2. Rühma $(G; \cdot)$ alamrühmaks nimetatakse hulka $H \subseteq G$, mille korral on täidetud kolm tingimust

$$\forall x, y \in H \qquad x \cdot y \in H \tag{4}$$

$$1 \in H \tag{5}$$

$$\forall x \in H \qquad x^{-1} \in H \tag{6}$$

Neid omadusi nimetatakse kinnisuseks korrutamise suhtes, kinnisuseks ühikelemendi võtmise suhtes ning kinnisuseks pöördelemendi võtmise suhtes.

Näide 4. Eelnevast teame, et $E = \{1\}$ on rühma $\mathbb{Q}^*$ alamrühm. See kehtib iga rühma korral, sest $1 \cdot 1 = 1$, mistõttu on tagatud kinnisus korrutamise ja ühikelemendi võtmise suhtes. Kuna $1^{-1} = 1$, siis on täidetud ka kinnisus pöördelemendi võtmise suhtes.

Näide 5. Vaatme arvu 5 jääkide hulka $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$, siis korrutamise suhtes on meil rühmad $E = \{1\}$, $H = \{1, 4\}$ ja $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$. Seega on E rühmade H ja $\mathbb{Z}_5^*$ alamrühm ning H on alamrühma $\mathbb{Z}_5^*$ alamrühm.

Kui rühmas on lõplik arv elemente, siis rühmaelementide arv määrab ära võimaliku alamrühma elementide arvu. Jätkates näidet toome sisse järgnevas tõestuses vajaliku kõrvalklasside mõiste

Definitsioon 3. Rühma G elemendi a vasakpoolseks kõrvalklassiks alamrühma H suhtes nimetatakse hulka $aH = \{ah \mid h \in H\}$.

Näide 6. Võttes rühmaks arvu 13 nullist erinevate jääkide hulga $\mathbb{Z}_{13}^*$ ning alamrühmaks $H = \{1, 3, 9\}$ saame kergesti leida kõikide elementide kõrvalklassid

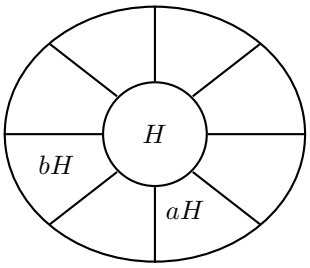
$$1H = 3H = 9H = \{1, 3, 9\} \qquad 4H = 10H = 12H = \{4, 10, 12\}$$
$$2H = 5H = 6H = \{2, 5, 6\} \qquad 7H = 8H = 11H = \{7, 8, 11\}$$

Nüüd on kogu vajalik matemaatiline masinavärk olemas, et tõestada järgnev teoreem.

Teoreem 1 (Lagrange' teoreem)**.** Iga lõpliku rühma alamrühma elementide arv jagab rühma elementide arvu.

Tõestus

Tähistame rühma G ja selle alamrühma H. Selleks jagame rühma omavahel lõikumatuteks osadeks tükkideks ning näitame, et igas tükis on täpselt samapalju elemente. Siis on tõestus valmis kuna oleme näidanud $|G| = t\,|H|$, kus t on tükelduses olevate tükkide arv. Iga elemendiga $a \in G$ on seotud kõrvalklass aH, seega kõik kõrvalklassid katavad kogu rühma G. Kui kahe kõrvalklassi aH ja bH ühisosa pole tühi, siis leidub element c nii, et



$$ah_1 = c = bh_2, \qquad h_1, h_2 \in H$$

Kuna h_1 on pööratav element, siis $a = ah_1h_1^{-1} = bh_2h_1^{-1} \in bH$, sest H on kinnine korrutamise ja pöördelemendi võtmise suhtes. Nüüd on selge, et $aH \subseteq bH$, sest iga korrutis $ah = (bh_2h_1^{-1})h = b(h_2h_1^{-1}h) \in bH$. Täpselt samasuguse tõestusega saab näidata $bH \subseteq aH$ ning seega $aH \cap bH \neq \emptyset \Rightarrow aH = bH$. See kindlustabki erinevate tükkide omavahelise lõikumatuse. Näitame veel, et igas tükis on samapalju elemente, selleks defineerime kujutuse $f : H \to aH$ järgneva reegli abil $f(h) = ah$. Paneme tähele, et see kujutab tõesti $f(H) \subseteq aH$ ja tänu a pööratavusele on kujutis injektiivne, sest $f(h_1) = ah_1 = ah_2 = f(h_2)$, siis korrutades võrdust a^{-1} saame $h_1 = h_2$. Kõrvalklassi definitsiooni järgi on f pealekujutus ning seega peab kehtima $|H| = |aH|$.
□

2 Pööratavate jääkide rühmad

Tänu laiendatud Eukleidese algoritmile saab iga jääki $a \in \mathbb{Z}_n$ pöörata parajasti siis, kui $\text{SÜT}(a, n) = 1$. Nüüd on lihtne veenduda, et pööratavate elementide hulk $U(\mathbb{Z}_n)$ on rühm korrutamise suhtes, sest kui $\text{SÜT}(a, n) = \text{SÜT}(b, n) = 1$, siis on seda ka $\text{SÜT}(ab, n)$ ja seega on arvule ab vastav jääk pööratav. Korrutamise assotsiatiivsus $(xy)z = x(yz)$ pärandub harilike täisarvude omadustest ja samamoodi on ühikuks jääk 1.

Olulisel kohal rühmade teoorias on ühe elemendi astmete poolt moodustatud rühmad

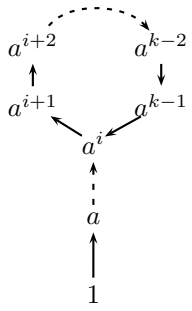
Definitsioon 4. Rühma G elemendi a poolt genereeritud rühmasks nimetatakse alamrühma $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$.

See on tõesti almrühm, sest $a^n \cdot a^m = a^{m+n}$ ja $a^n \cdot a^{-n} = a^0 = 1$. Seega sarnaselt arvudega astme a^n pöördelemendiks $\left(a^n\right)^{-1} = a^{-n}$.

Lemma 1. Kui rühm G on lõplik, siis iga tema elemendi a poolt genereeritud alamrühm on kujul $\langle a \rangle = \{1, a, a^2, \ldots, a^{k-1}\}$, kusjuures $a^k = 1$.

Tõestus

Vaatleme ahelat $1 \to a \to a^2 \to a^3 \to \cdots$, kuna rühm on lõplik, siis tekib mingil sammul astmeks selline element a^i, mis on ahelas juba olemas. Lihtne on taibata, et edasisel astendamisel saame vastavalt a^{i+1}, a^{i+2} jne. Põhimõtteliselt on võimalik järgmine pilt. Järgnevalt näitame, et see pole võimalik, st. $a^k = 1$. Oletame, et meil tekib saba, siis leidub $0 < i$ nii, et $a^i = a^k$, kuid samas $a^{i-1} \neq a^{k-1}$. Kohe saame vastuolu, sest $a^{i-1} = a^{-1}a^i = a^{-1}a^k = a^{k-1}$. Kuna vastuolu tekkis, sellest et eeldasime $0 < i$, siis peab $i = 0$. Siis mingit vastuolu ei teki, kuna me ei saa ahelas ühte sammu tagasi teha. Seega $a^k = a^0 = 1$.



□

Näide 7. Näiteks arvu 27 jääkide hulga $\mathbb{Z}_{27}$ pööratavad elemente on 18

$$U(\mathbb{Z}_{27}) = \{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26\}$$

ja seega saaks põhimõtteliselt olemas olla alamrühmi, milles on 1, 2, 3, 6 või 9 elementi. Vaatleme nüüd alamrühmi, mis on moodustatud ühe jäägi astmete poolt, mugavuse mõttes on jäägid järjestatud suuruse järjekorras

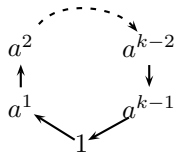
$$\begin{aligned}
\langle 2\rangle &= \langle 5\rangle = \langle 11\rangle = \langle 14\rangle = \langle 20\rangle = \langle 23\rangle \\
\langle 2\rangle &= \{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26\} \\
\langle 4\rangle &= \langle 7\rangle = \langle 13\rangle = \langle 16\rangle = \langle 22\rangle = \langle 25\rangle \\
\langle 4\rangle &= \{1, 4, 7, 10, 13, 16, 19, 22, 25\} \\
\langle 8\rangle &= \{1, 8, 10, 17, 19, 26\} \\
\langle 10\rangle &= \langle 19\rangle = \{1, 10, 19\} \\
\langle 26\rangle &= \{1, 26\}
\end{aligned}$$

Nüüd on lihtne tõestada järgmist fundamentaalset teoreemi.

Teoreem 2 (Euleri teoreem)**.** Iga pööratava elemendi $a \in U(\mathbb{Z}_n)$ korral kehtib kongurentside võrdus $a^{\phi(n)} \equiv 1 \mod n$.

Tõestus

Vaatme suvalist pööratavat elementi $a \in U(\mathbb{Z}_n)$ ning selle poolt moodustatud alamrühma $\langle a\rangle$. Lemma 1 tõttu peab $a^k \equiv 1 \mod n$, kus k on alamrühma $\langle a\rangle$ elementide arv. Lagrange' teoreemi tõttu peab k jagama pööratavate jääkide arvu $\phi(n) = |U(\mathbb{Z}_n)|$. Formaalselt tähendab see $lk = \phi(n)$ ja seega $a^{\phi(n)} \equiv \left(a^k\right)^l \equiv 1^l \equiv 1 \mod n$.



□

3 Nullitegurid

Mõnikord on olemas peale ühikelelemendi 1 ka nullelement 0, millega igat teist elementi vasakult ja paremalt korrutades on tulemuseks 0. Sarnaselt ühikelemendile saab seda olla sammuti vaid üks. Rühmas, milles on rohkem kui üks element ei saa nullelementi olla, sest kui $1 \neq 0$, siis ei saa leida 0^{-1}. Kui me vaatme jääke $\mathbb{Z}_n$ korrutamise suhtes, siis on seal nullelement ja see on 0. Kui mõelda, siis 0 on olemas alati tegurid $a0 = 0$, aga selline teguriteks lahutus on triviaalne, seepärast defineeritakse nullitegurid eraldi.

Definitsioon 5. Nulliteguriteks nimetatakse nullist erinevaid elemente a ja b, mille korrutis $a \cdot b = 0$.

Kuna pea kõikides rühmades ei esine 0 ja nullitegureid, siis peame täpsustama, milliseid omadusi me korrutustehtelt nõuame ja see viib formaalsete definitsioonideni.

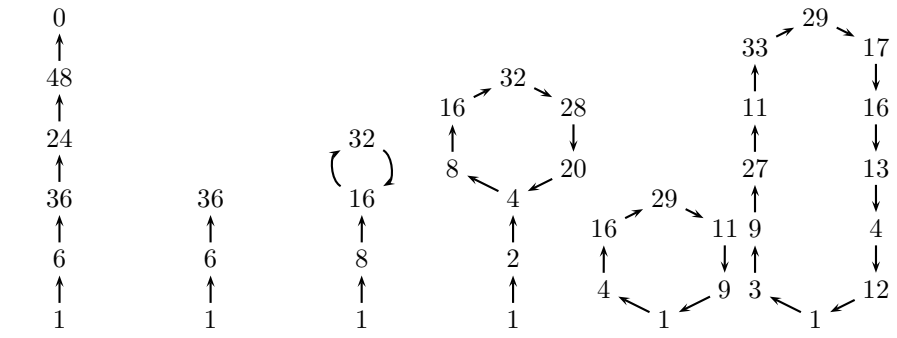
Definitsioon 6. Poolrühmaks nimetatakse hulka R, millel on defineeritud kahekohaline funktsioon(tehe) $\bullet(\cdot,\cdot) : R \times R \to R$, mis rahuldab järgmist tingimust

$$\forall x, y, z \in R \quad (x \cdot y) \cdot z = x \cdot (y \cdot z). \tag{7}$$

Kui alamhulk $A \subseteq R$ on kinnine korrutamise suhtes, siis nimetatakse seda alampoolrühmaks.

Sama moodi saab vaadata poolrühmades elemendi a astmete poolt moodustatud alampoolrühmi. Kuna meil ei pruugi leiduda a pöördelemendi ja ühikelementi, siis tähistatakse $\langle a \rangle = \{a^k \mid k \in \mathbb{N}\}$. Kui poolrühmas leidub ühikelement, siis lisatakse see hulka $\langle a \rangle$.

Näide 8. Eelenevalt vaadeldud jääkide hulgad $\mathbb{Z}_n$ on korrutamise suhtes poolrühmad. Toome näiteteid mõningate erinevate arvude jääkide alampoolrühmadest. Kui poolrühm on lõplik, siis mingil hetkel tekib astmete hulka selline element, mis on juba olnud. Kuid erinevalt rühmast ei pruugi alati tekkida tsükel. Üldjuhul tekib sabaga tsükkel, kuid on võimalikud ka teised võimalused.



$\langle 6 \rangle \subseteq \mathbb{Z}_{96}$ $\langle 6 \rangle \subseteq \mathbb{Z}_{60}$ $\langle 8 \rangle \subseteq \mathbb{Z}_{48}$ $\langle 2 \rangle \subseteq \mathbb{Z}_{36}$ $\langle 4 \rangle \subseteq \mathbb{Z}_{35}$ $\langle 3 \rangle \subseteq \mathbb{Z}_{35}$

4 Hiina jäägiteoreem ja RSA korrektsus

Kuna RSA-s kasutatakse moodulina kahe algarvu korrutist, siis on meil kasulik teada, kuidas esitada jääke võimalikult kompaktselt. Üks võimalus on kasutada vanade hiinlaste poolt tõestatud Hiina jäägiteoreemi

Teoreem 3 (Hiina jäägiteoreem)**.** Kui täisarvud m ja n on ühistegurita, siis iga kongurentside süsteem

$$\begin{aligned} x &\equiv a \mod m \\ x &\equiv b \mod n \end{aligned}$$

on lahenduv ning lahend on ühene mooduli mn järgi.

Tõestus

Esmalt paneme tähele, et negatiivsete arvude jäägid on samad, mis nendele vastavatel positiivsetel arvudel. Kui üks arvudest m ja n on null, siis suurim ühistegur on teine arv ning seega pole m ja n ühistegurita. Nüüd paneme tähele, et kuna $\text{SÜT}(m, n) = 1$, siis laiendatud Eukleidese algoritm annab meile arvud c ja d nii, et

$$\begin{aligned} dn &\equiv 1 \mod m \\ cm &\equiv 1 \mod n \end{aligned}$$

Nüüd leides arvudele cn ja dm vastavad jäägid e_1 ja e_2 mooduli mn järgi saame

$$\begin{aligned} e_1 &\equiv dn \equiv 1 \mod m & \qquad e_2 &\equiv cm \equiv 0 \mod m \\ e_1 &\equiv dn \equiv 0 \mod n & \qquad e_2 &\equiv cm \equiv 1 \mod n \end{aligned}$$

sest arvu jääki n järgi võib leida nii, et esmalt leiame arvu jäägi mn järgi ja siis omakorda selle jäägi n järgi. Tulemus on õige, sest mn jagub arvuga n. Võttes nüüd arvuks x arvu $ae_1 + be_2$ jäägi mooduli mn järgi on rahuldatud mõlemad võrdused, sest

$$\begin{aligned} x &\equiv e_1a + e_2b \equiv 1a + 0b \equiv a \mod m \\ x &\equiv e_1a + e_2b \equiv 0a + 1b \equiv b \mod n \end{aligned}$$

Lahendi ühesuseks paneme tähele, et iga arvupaari (a, b), kus $a \in \mathbb{Z}_m$ ja $b \in \mathbb{Z}_n$ korral leidub meil vähemalt üks lahend mooduli mn järgi. Kokku on arvupaare $m \times n$ ja jääke mooduli mn järgi $m \times n$. Igale jäägile x saab vastata vaid üks arvupaar (a, b), seega kui mõnele paarile (a, b) vastaks mitu jääki, siis peaks lahendite arv olema suurem kui $m \times n$, mis on ilmne vastuolu. Seetõttu on lahend ühene mooduli mn järgi.
□

Näide 9. Vaatame arvu 12 jääke. Kuna $12 = 4 \cdot 3$, siis iga jäägi $x \in \mathbb{Z}_{12}$ asemele võime kirjutada paari (a, b), kus $a \in \mathbb{Z}_4$ ja $b \in \mathbb{Z}_3$. Näiteks jäägile 5 vastab $(1, 2)$ ja 8 vastab $(0, 2)$. Lihtne on veenduda, et $13 = 5 + 8$ vastab

$$(1, 1) = (1 + 0, 2 + 2) = (1, 2) + (0, 2)$$

ja $40 = 5 \cdot 8$ vastab

$$(0, 1) = (1 \cdot 0, 2 \cdot 2) = (1, 2) \cdot (0, 2).$$

See tähelepanek on sissejuhatuseks järgmisele järeldusele.

Järeldus 3.1. Kui arvud m ja n on ühistegurita, siis võib iga jäägi hulgast $\mathbb{Z}_{mn}$ panna kirja paarina (a, b), kus $a \in \mathbb{Z}_m$ ja $b \in \mathbb{Z}_n$. Kusjuures see tähistus on kooskõlas liitmise ja korrutamisega, st. kehtivad seosed

$$\begin{aligned}(a, b) + (c, d) &\equiv (a + c, b + d) \mod mn \\ (a, b)(c, d) &\equiv (ac, bd) \mod mn\end{aligned}$$

Tõestus

Tõestuseks on tarvis tähele panna vaid seda, et kui $x + y \equiv z \mod mn$, siis kehtivad $x + y \equiv z \mod m$ ja $x + y \equiv z \mod n$. Tänu hiina jäägiteoreemile saab z üheselt määrata kongurentside süsteemist

$$\begin{aligned}x + y &\equiv z \mod m \\ x + y &\equiv z \mod n\end{aligned}$$

See põhjendab esimese võrduse. Analoogne põhjendus on aluseks teisele võrdusele.
□

Nüüd saame väga lihtsalt kasutades hiina jäägiteoreemi tõestada RSA korrektsust tagava teoreemi.

Teoreem 4 (RSA korrektsus)**.** Kui arv n lahutub kahe erineva algarvu p ja q korrutiseks, siis iga jäägi x ja astendajate a ja b korral, mis rahuldavad tingimusi $ab \equiv 1 \mod \phi(n)$, kehtib võrratus

$$x^{ab} \equiv x \mod n.$$

Tõestus

Kuna p ja q on ühistegurita, siis saame kasutada hiina jäägiteoreemi järeldust 3.1, st me võime vaadata x vastavat jääkide paari (x_1, x_2), kus $x_1 \in \mathbb{Z}_p$ ja

$x_2 \in \mathbb{Z}_q$, siis saame kirjutada välja järgmised võrduste ahela

$$(x_1, x_2)^{k\phi(n)+1} \equiv (x_1, x_2)^{k(p-1)(q-1)+1} \equiv \left(x_1^{k(p-1)(q-1)+1}, x_2^{k(p-1)(q-1)+1}\right) \equiv$$
$$\left(x_1 \cdot \left(x_1^{p-1}\right)^{k(q-1)}, x_2 \cdot \left(x_2^{q-1}\right)^{k(p-1)}\right) \equiv (x_1, x_2) \mod n$$

sest sulgude sees saame kasutada Euleri teoreemi ja fakti $\phi(p) = p - 1$ ja $\phi(q) = q - 1$. See tõestus on korrektne nii, pööratavate kui mittepööratavate jääkide korral. Kui x on pööratav, siis lihtne järeldus Euleri teoreemist annab sama tulemuse

$$x^{k\phi(n)+1} \equiv \left(x^{\phi(n)}\right)^k x \equiv x \mod n$$

Kuid siis tuleks võrdus eraldi tõestada ka mittepööratavate elementide korral. See on tehniliselt samaväärne esimese võrduste ahelaga.
□

5 Fermat' väike teoreem, mittetriviaalsed ruutjuured ja algarvu testid

Algarvude tuvastamine kuulub korraga keerukusklassidesse $\mathcal{NP}$ ja $co - \mathcal{NP}$ ning siiani pole leitud ühtegi rangelt determineeritud algoritmi, mis töötaks polünomiaalses ajas kontrolitava arvu pikkusest. Ometi on praktilistes rakendustes vaja suuri algarve suurusjärku 256-512 bitti pikad. Osaliselt annab sellele vastuse järgnev teoreem.

Teoreem 5 (Fremat' väike teoreem)**.** Kui p on algarv, siis iga jäägi a korral kehtib võrratus $a^p \equiv a \mod p$.

Tõestus

Nulli korral kehtib võrdus igal juhul ning kuna ainuke mittepööratav jääk mooduli p järgi on 0, siis $\phi(p) = p - 1$ ja seega iga nullist erineva jäägi korral

$$a^p \equiv \left(a^{\phi(p)}\right) a \equiv a \mod p.$$

□

Seega kui leidub mõni nullist erinev jääk a, mille korral $a^{n-1} \not\equiv 1 \mod n$, siis on see tõestus selle kohta, et n pole algarv. Seega lihtsaim algarvu test on järgmine

Fermat' algarvu test

Sisend on arv n

1. Valida juhuslikult $a \in \{2, ...n-2\}$
2. Arvutada $b \equiv a^{n-1} mod n$
3. Kui $b \not\equiv 1 \mod n$, siis väljastada KORDARV, muidu ALGARV.

Kui n on algarv, siis töötab algoritm korrektselt, kuid mõne n korral võib valida a selliselt, et $a^{n-1} \equiv 1 \mod n$, kuigi n pole algarv. Selliseid ühest ja miinus ühest erinevaid jääke nimetatakse Fermat' valetajateks. Kui a on mittepööratav, siis on ilmne $a^{n-1} \not\equiv 1$, õnnetuseks on mittepööratavaid jääke tühiselt vähe, kui n tegurid on suured. On näidatud, et algoritmi vea tõenäosus on enamiku kordarvude korral ligikaudu 1/2.

Näide 10. Vaatame näiteks arvu 21 jääke, siis Fermat valetajad on 8 ja 13. Arvu 45 Fermat' valetajad on 8, 17, 19, 26, 28 ja 37. Nagu näitest näha on, siis võib mõne arvu korral olla palju Fermat valetajaid, seega oleks vaja veidi täpsemat algoritmi. Leidub koguni arve *Charmichaeli* arvud, millel ei leidu ühtegi pööratavat Fermat' tunnistajat vähim selline on 561.

Seega on meil tarvis mingit efektiivsemat kriteeriumi kordarvude avastamiseks. Üks võimaliku vastuse pakub järgmine lemma.

Lemma 2. Kui n on algarv, siis ainsad jäägid, mis rahuldavad kongurentside süsteemi $x^2 \equiv 1 \mod n$ on 1 ja $n-1$.

Tõestus

Ilmne teisendus näitab, et kongusrentside süsteem on samaväärne

$$(x+1)(x-1) \equiv x^2 - 1 \equiv 0 \mod n.$$

Kuna n on algarv, siis peab ta jagama $x+1$ või $x-1$ ainsad võimalikud jäägid on seega tõesti 1 ja $n-1$.
□

Sellel lemmal põhine Rabin-Milleri algarvu test.
Rabin-Milleri algoritm

Sisend arv n

1. Avaldada $n-1 = 2^k m$, kus m on paaritu.
2. Valida juhuslikult $a \in \{2, ..., n-2\}$.
3. Arvutada $b \equiv a^m \mod n$.
4. Kui $b \equiv 1 \mod n$, siis väljastada ALGARV.
5. for i $= 0, 1, .., k-1$ do

Kui $b \equiv -1 \mod n$, siis väljastada ALGARV, muidu $b \equiv b^2 \mod n$.

6. Väljastada KORDARV.

Kui n on algarv, siis $a^{n-1} \equiv 1 \mod n$ ja seega arvestades lemmat 2 on selge, et kas $a^m \equiv 1 \mod n$ või leidub jadas $a^m, a^{2m}, \cdots, a^{2^{k-1}m}$ element, mis on kongurentne $n-1$, sest ainsad ühe ruutjuured on 1 ja $n-1 \equiv -1 \mod n$. On lihtne tähele panna, et see on täiustatud Fermat' test, st. kui Rabin-Milleri algoritm väljastab algarv, siis teeb seda ka Fermat' test. Kuid mõnede Fermat' valetajate korral suudab Rabin-Milleri algoritm need paljastada. Kui jadas $a^m, a^{2m}, \cdots, a^{2^{k-1}m}$ on mittetriviaalne ühe ruutjuur b, siis ei väljastata, selle

korral ALGARV ning pärast seda ka mitte, sest $b^{2^i} \equiv 1 \not\equiv -1 \mod n$. Seetõttu on lõpptulemuseks väljund KORDARV. See viib vea tõenäosuse, et kordarvu korral väljastatakse algarv, alla ning see on ligikaudu 1/4. Ning algoritm võidab ühtlasi ka *Charmichaeli* arvud.

Näide 11. Vaatme arvu 21 Fermat' valetajatele vastavaid jadasid a, a^5, a^{10} ja a^{20} ning sellele vastavat väljundit

$$\begin{aligned} 8 &\to 8 \to 1 \to 1 \Rightarrow \text{KORDARV} \\ 13 &\to 13 \to 1 \to 1 \Rightarrow \text{KORDARV} \end{aligned}$$

Sama moodi arvutades a, a^{11}, a^{22} ja a^{44} saab paljastada kõik arvu 45 Fermat' valetajad

$$\begin{aligned} 8 &\to 17 \to 19 \to 1 \Rightarrow \text{KORDARV} \\ 17 &\to 8 \to 19 \to 1 \Rightarrow \text{KORDARV} \\ 19 &\to 19 \to 1 \to 1 \Rightarrow \text{KORDARV} \\ 26 &\to 26 \to 1 \to 1 \Rightarrow \text{KORDARV} \\ 28 &\to 37 \to 19 \to 1 \Rightarrow \text{KORDARV} \\ 37 &\to 28 \to 19 \to 1 \Rightarrow \text{KORDARV} \end{aligned}$$

Näiteks ebaõnnestumise kohta võib vaadata arvu 25 Fermat'i valetajaid 7 ja 18

$$\begin{aligned} 7 &\to 18 \to -1 \Rightarrow \text{ALGARV} \\ 18 &\to 7 \to -1 \Rightarrow \text{ALGARV} \end{aligned}$$

Fermat' ja Rabin-Milleri test on sama keerukusega $\mathcal{O}(\log^3 n)$, see ei määra algarvu leidmise keerukust, sest test näitab vaid kas arv on algarv või mitte. Algebralistel põhjusel on tõenäosus, et arv n on algarv ligikaudu $1/\log n$, seega keskmiselt tuleb testida $\mathcal{O}(\log n)$ arvu, mistõttu kulub keskmiselt $\mathcal{O}(\log^4 n)$ operatsiooni, et saada sobiva suurusega algarv. See on suurte arvu pikkuste korral probleem väiksema võimsusega arvutitele.