

# Calculus<sup>Lukion</sup>

Täydentävä aineisto

Alkuluvut 2, 3, 5, 7, 11, 13, 17, ...,  $2^{43112609}-1, \dots$

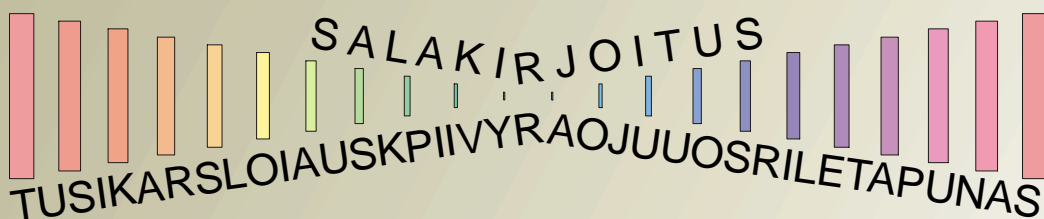


$\text{sy}(a,b)$

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

$\text{py}(a,b)$

$$ab = \text{sy}(a,b) \cdot \text{py}(a,b)$$



## LUONNOLLISTEN LUKUJEN JAOLLISUUS

Paavo Jäppinen  
Alpo Kupiainen  
Matti Räsänen

# Luonnollisten lukujen jaollisuus

Luonnollisten lukujen joukko  $\mathbf{N}$  koostuu kokonaisluvuista 0, 1, 2, 3, ... eli positiivisista kokonaisluvuista ja luvusta nolla.

$$\mathbf{N} = \{0, 1, 2, 3, \dots\}$$

Luonnollisia lukuja on alun perin käytetty ilmaisemaan lukumäärää tai järjestystä. Minkä tahansa kahden luonnollisen luvun summa ja tulo ovat myös luonnollisia lukuja. Tähän perustuen sanotaan, että yhteenlasku ja kertolasku ovat määriteltyjä joukossa  $\mathbf{N}$ .

## 1 Jaollisuussääntöjä

Sovitaan aluksi, että tässä esityksessä pienet kirjaimet  $a, b, c, \dots$  tarkoittavat luonnollisia lukuja. Jakajana oleva luku ei saa olla nolla. Jos luku  $a$  voidaan esittää muodossa  $a = bc$ , sanotaan, että  $b$  on  $a$ :n tekijä ja merkitään  $b \mid a$ . Käytetään myös sanontaa  $b$  jakaa  $a$ :n tai  $a$  on jaollinen  $b$ :llä, kun  $b \neq 0$ . Merkintä  $d \nmid a$  puolestaan ilmaisee, että  $d$  ei ole  $a$ :n tekijä.

Esimerkiksi luku 55 voidaan esittää tulona  $55 = 5 \cdot 11$ , josta käy ilmi, että luku 55 on jaollinen luvuilla 5 ja 11 eli  $5 \mid 55$  ja  $11 \mid 55$ . Sen sijaan 55 ei ole jaollinen seitsemällä eli  $7 \nmid 55$ , koska osamäärä  $55 : 7$  ei ole luonnollinen luku.

### Esimerkki 1

a)  $6 \mid 30$ , koska  $6 \cdot 5 = 30$ .

b)  $5 \nmid 93$ , koska osamäärä  $93 : 5 (= 18,6)$  ei ole luonnollinen luku.

c) Luvun 12 tekijöinä ovat luonnolliset luvut 1, 2, 3, 4, 6 ja 12.

d) Luvulla 5 jaollisten luonnollisten lukujen joukko on  $\{0, 5, 10, 15, 20, \dots\}$ . Nämä luvut ovat muotoa  $5n$ , jossa  $n$  on luonnollinen luku. Parillisten lukujen esitys on vastaavasti  $2n$  ja parittomien  $2n + 1$ .

Luonnollisten lukujen jaollisuus toisella luonnollisella luvulla on aina mahdollista selvittää jakolaskulla. Usein jaollisuus on kuitenkin helpointa ratkaista käyttämällä kymmenjärjestelmän jaollisuussääntöjä. Säännöt helpottavat luvun jakamista tekijöihin.

Luonnollinen luku on jaollinen

*kahdella*, jos sen viimeinen numero on 0, 2, 4, 6 tai 8

*kolmella*, jos sen numeroiden summa on jaollinen kolmella

*neljällä*, jos sen kahden viimeisen numeron muodostama luku on jaollinen neljällä

*viidellä*, jos sen viimeinen numero on 0 tai 5

*kuudella*, jos se on jaollinen kahdella tai kolmella

*kahdeksalla*, jos sen kolmen viimeisen numeron muodostama luku on jaollinen kahdeksalla

*yhdeksällä*, jos sen numeroiden summa on jaollinen yhdeksällä

*kymmenellä*, jos sen viimeinen numero on 0

Edellä esitetyt jaollisuussäännöt ovat tavallisimmat ja monet niistä ennestään tuttuja. Näiden lisäksi tarkastellaan seuraavassa esimerkissä lähinnä erikoisuutena esimerkin avulla *seitsemällä* ja *yhdellätoista* jaollisuutta.

### Esimerkki 2

Luonnollisen luvun jaollisuus seitsemällä ja yhdellätoista.

#### a) Seitsemällä jaollisuus

Luvun 9 625 seitsemällä jaollisuus testataan seuraavalla tavalla:

Poistetaan luvun viimeinen numeromerkki (5) ja vähennetään jäljelle jäävästä luvusta (962) poistettu numero kahdella kerrottuna ( $962 - 2 \cdot 5 = 952$ ). Jatketaan samalla tavalla eli poistetaan viimeinen numero (2) ja vähennetään jäljelle jäävästä luvusta (95) poistettu luku kahdella ( $95 - 2 \cdot 2 = 91$ ). Viimeksi saadusta muodosta voidaan seitsemällä jaollisuus päätellä ( $91 = 7 \cdot 13$ ) tai haluttaessa jatketaan vielä yksi askel ( $9 - 2 \cdot 1 = 7$ ).

#### b) Yhdellätoista jaollisuus

Luvun 140 349 jaollisuus yhdellätoista selvitetään seuraavalla tavalla:

Lasketaan ensin järjestyksessä parittomien (ensimmäinen, kolmas, viides jne.) numeromerkkien summa:  $1 + 0 + 4 = 5$ .

Vastaavalla tavalla lasketaan järjestyksessä parillisten (toinen, neljäs, kuudes jne.) numeromerkkien summa:  $4 + 3 + 9 = 16$ .

Mikäli edellä saatujen summien erotus on nolla tai yhdellätoista jaollinen, tutkittava luku on jaollinen yhdellätoista.

Koska esimerkin tapauksessa erotus on 11 (tai vähennysjärjestystä vaihtaen  $-11$ ), luku 140 349 on jaollinen luvulla yksitoista.

### Esimerkki 3

Nelinumeroinen luonnollinen luku voidaan esittää muodossa  $1\,000a + 100b + 10c + d$ , jossa kirjaimet  $a, b, c$  ja  $d$  vastaavat kymmenjärjestelmän numeromerkkejä 0, 1, 2, ..., 9. (Esim.  $4\,321 = 4 \cdot 1\,000 + 3 \cdot 100 + 2 \cdot 10 + 1$ )

Osoita, että tätä muotoa oleva luku on jaollinen kolmella (yhdeksällä), jos numeromerkkien  $a, b, c$  ja  $d$  summa on jaollinen kolmella (yhdeksällä).

*Ratkaisu:*

Luku  $1\,000a + 100b + 10c + d$  voidaan kirjoittaa muotoon

$$(999a + a) + (99b + b) + (9c + c) + d$$

ja edelleen

$$(999a + 99b + 9c) + (a + b + c + d).$$

Helposti nähdään, että ensimmäinen summalauseke on jaollinen kolmella (yhdeksällä). Alkuperäinen luku on näin ollen jaollinen kolmella (yhdeksällä), jos myös jälkimmäinen summalauseke on jaollinen kolmella (yhdeksällä).

Edellä mainittu luku 4 321 ei ole jaollinen kolmella eikä yhdeksällä, koska numeromerkkien summa on 10.

Esimerkissä 3 käytettiin hyväksi seuraavaa jaollisuuslauseetta:

Jos  $k \mid a$  ja  $k \mid b$ , niin  $k \mid (a + b)$ . (Summassa voi olla useampiakin yhteenlaskettavia.)

*Todistus:*

Oletuksen perusteella on olemassa luvut  $r$  ja  $s$  niin, että  $a = rk$  ja  $b = sk$ . Tällöin

$$a + b = rk + sk = k(r + s),$$

josta lauseen väite nähdään oikeaksi. Todistus on vastaavanlainen, jos yhteenlaskettavia on useampia kuin kaksi. Koska erotus voidaan esittää summana, esimerkiksi  $a - b = a + (-b)$ , jaollisuuslause pätee myös erotukselle.

Summan jaollisuusominaisuuksiin liittyy läheisesti myös seuraava lause:

Jos summan yhteenlaskettavat yhtä lukuun ottamatta ovat jaollisia samalla luvulla, niin summa ei ole jaollinen tällä luvulla.

*Todistus:*

Olkoon  $s = b + c$  ja  $a \mid b$  mutta  $a \nmid c$ . Tällöin myös  $a \mid -b$ . Jos nyt olisi  $a \mid s$ , niin edellisen lauseen mukaan  $a \mid (s - b)$  eli  $a \mid c$ . Tämä on kuitenkin vastoin lauseen oletusta, joten summa ei ole jaollinen  $a$ :lla. Todistus on vastaava, jos yhteenlaskettavia on enemmän kuin kaksi.

## Lohkaisuperiaate

Luonnollisen luvun jaollisuutta voidaan tutkia myös ns. *lohkaisuperiaatteella*, joka perustuu edellä todistettuihin lauseisiin. Tutkittava luku esitetään kahden luvun summana siten, että edellisestä yhteenlaskettavasta jaollisuus nähdään helposti. Tällöin koko luvun jaollisuus jää riippumaan jälkimmäisen yhteenlaskettavan jaollisuudesta.

### Esimerkki 4

Tutki suorittamatta jakolaskua, onko luku 50 695 864 on jaollinen neljällä.

*Ratkaisu:*

Luku 50 695 864 ”lohkaistaan” muotoon  $50\,695\,800 + 64 = 506\,958 \cdot 100 + 64$ . Saadun summan kumpikin yhteenlaskettava on jaollinen neljällä, koska  $100 = 25 \cdot 4$  ja  $64 = 16 \cdot 4$  (ks. tehtävä 7). Tällöin myös summa eli annettu luku on jaollinen neljällä.

Vähintään kaksinumeroinen kokonaisluku voidaan aina kirjoittaa summana äsken esitetyllä tavalla. Jos nyt kahden viimeisen numeron muodostama luku on neljällä jaollinen, koko luku on neljällä jaollinen. Tämä on juuri sivulla 1 esitetty neljällä jaollisuuden sääntö. Vastaavasti saadaan kahdeksalla jaollisuuden sääntö vähintään kolminumeroisille luvuille.

### Esimerkki 5

Osoita jakolaskua suorittamatta, että luku 350 015 ei ole jaollinen seitsemällä.

*Ratkaisu:*

Kirjoitetaan  $350\,015 = 350\,000 + 15$ . Summan ensimmäinen yhteenlaskettava on jaollinen seitsemällä, sillä  $350\,000 = 50\,000 \cdot 7$ . Mutta koska toinen yhteenlaskettava ei ole seitsemällä jaollinen, ei myöskään annettu luku ole seitsemällä jaollinen.

## Tehtäviä

Tehtävät 1–6 on tarkoitettu laskettavaksi ilman laskinta.

1. Tutki, pitääkö väite paikkansa. Perustelee!  
a)  $2 \mid 1\,503$       b)  $6 \nmid 1\,565$       c)  $5 \mid 72\,000$       d)  $7 \mid 4\,214$
2. Kuinka monta eri suurta tekijää on luvulla 1 000?
3. Mitkä seuraavista luvuista ovat jaollisia neljällä?  
a) 434                  b) 2 444                  c) 11 036                  d) 630 254
4. Tutki luvun jaollisuutta seitsemällä.  
a) 787                  b) 1 001                  c) 3 300                  d) 332 640
5. Mitkä seuraavista luvuista ovat jaollisia yhdellätoista?  
a) 11 111                  b) 271 590                  c) 72 011                  d) 171 028
6. Selvitä, onko luku 234 567 890 136 jaollinen annetulla luvulla.  
a) 2                      b) 3                      c) 4                      d) 5  
e) 6                      f) 7                      g) 8                      h) 9  
i) 10                      j) 11
7. Todista, että kahden luvun tulo on jaollinen tietyllä luvulla, jos ainakin toinen tekijä on jaollinen tällä luvulla.
8. Etsi kaikki kolminumeroiset luonnolliset luvut, jotka ovat jaollisia sekä luvulla 7 että luvulla 11.
9. Tutki lohkaisuperiaatetta käyttäen, onko  
a) luku 49 1049 jaollinen seitsemällä  
b) luku 99 011 jaollinen yhdellätoista

## 2 Alkuluvut

Luonnollista lukua, joka on vähintään 2, sanotaan *alkuluvuksi* eli *jaottomaksi luvuksi*, jos se ei ole jaollinen muilla positiivisilla luvuilla kuin itsellään ja luvulla yksi. Kaikki muut lukua 2 suuremmat luonnolliset luvut ovat *yhdistettyjä* lukuja.

Vanha keino etsiä alkulukuja on käyttää *Eratostheneen seula*.

Esimerkiksi lukua 60 pienemmät alkuluvut etsitään seuraavasti:

Kirjoitetaan aluksi taulukkoon kaikki luvut kahdesta kuuteenkymmeneen. Ensimmäinen luku 2 on alkuluku. Yliviivataan kaikki muut kahdella jaolliset luvut. Luku 3 on seuraava alkuluku. Yliviivataan kaikki muut kolmella jaolliset luvut. Näin jatketaan etsimällä ensin seuraava alkuluku ja sitten yliviivaamalla sen monikerrat. Kun yliviivausta jatketaan siihen asti, kunnes tullaan alkulukuun, joka on suurempi tai yhtä suuri kuin  $\sqrt{60}$ , jäljelle jääneet ovat kaikki alkulukuja. Nimittäin jokainen yhdistetty luku, joka on pienempi tai yhtä suuri kuin 60, on jaollinen jollakin alkuluvulla  $p \leq \sqrt{60}$ . Mutta kaikki tällaiset luvut on jo yliviivattu.

	2	3	<del>4</del>	5	<del>6</del>	7	<del>8</del>	<del>9</del>	<del>10</del>
11	<del>12</del>	13	<del>14</del>	<del>15</del>	<del>16</del>	17	<del>18</del>	19	<del>20</del>
<del>21</del>	<del>22</del>	23	<del>24</del>	<del>25</del>	<del>26</del>	27	<del>28</del>	29	<del>30</del>
31	<del>32</del>	<del>33</del>	<del>34</del>	<del>35</del>	<del>36</del>	37	<del>38</del>	<del>39</del>	40
41	<del>42</del>	43	<del>44</del>	<del>45</del>	<del>46</del>	47	<del>48</del>	<del>49</del>	50
<del>51</del>	<del>52</del>	53	<del>54</del>	<del>55</del>	<del>56</del>	<del>57</del>	<del>58</del>	59	<del>60</del>

Esimerkissä riitti, kun yliviivattiin vain luvuilla 2, 3, 5 ja 7 jaolliset luvut, sillä seuraava alkuluku 11 on suurempi kuin  $\sqrt{60} \approx 7,7$ . Näin löydettiin lukua 60 pienemmät alkuluvut 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53 ja 59.

### Esimerkki 1

Tutki, onko luku 263 alkuluku.

*Ratkaisu:*

Jos 263 on yhdistetty luku, se on jaollinen jollakin alkuluvulla, joka on enintään  $\sqrt{263}$ .

Tällaisia tutkittavia alkulukuja ovat 2, 3, 5, 7, 11 ja 13, sillä  $\sqrt{263} \approx 16,2$ .

$$\begin{aligned} 263 : 2 &= 131,5, \text{ jakojäännös } 1 \\ 263 : 3 &= 87,666\ldots, \text{ jakojäännös } 2 \\ 263 : 5 &= 52,6, \text{ jakojäännös } 3 \\ 263 : 7 &= 37,571\ldots, \text{ jakojäännös } 4 \\ 263 : 11 &= 23,9, \text{ jakojäännös } 10 \\ 263 : 13 &= 20,23, \text{ jakojäännös } 3 \end{aligned}$$

*Huomautus:* Jaollisuutta tutkittaessa voidaan soveltaa myös aikaisemmin esitettyjä jaollisuussääntöjä.

Koska 263 ei ole millään tutkittavista luvuista jaollinen, se on alkuluku.

*Vastaus:* Luku 263 on alkuluku.

Alkuluku on jaoton, mutta yhdistetty luku voidaan jakaa tekijöihin usein monellakin eri tavalla. Esimerkiksi  $126 = 6 \cdot 21 = 3 \cdot 42 = 7 \cdot 18$  jne. Sitä vastoin on vain yksi tapa esittää yhdistetty luku alkulukujen tulona eli jakaa luku *alkutekijöihin*, jollei tekijöiden järjestystä oteta huomioon. On voimassa *aritmetiikan peruslause*:

### Aritmetiikan peruslause

Jokainen yhdistetty luonnollinen luku voidaan esittää vain yhdellä tavalla alkulukujen tulona, kun tekijöiden erilaista järjestystä ei oteta huomioon.

Määritelmänsä mukaan yhdistetty luonnollinen luku voidaan esittää kahden pienemmän luonnollisen luvun tulona. Jos nämä luvut eivät ole alkulukuja, ne voidaan edelleen esittää pienempien luonnollisten lukujen tulona. Kun näin jatketaan, yhdistetty luonnollinen luku saadaan jaetuksi alkutekijöihinsä.

Edellä olleen esimerkkiluvun 126 alkutekijäesitys  $2 \cdot 3 \cdot 3 \cdot 7$  eli  $2 \cdot 3^2 \cdot 7$  on aritmetiikan peruslauseen mukaan kyseisen luvun ainoa alkutekijäesitys.

### Tehtäviä

10. Jatka edellä esitettyä Eratostheneen seula lukuun 100 saakka. Mitkä luvut ovat alkulukuja välillä 2–100?
11. Kuinka monta parillista alkulukua on olemassa?
12. Jaa luvut alkutekijöihin.  
a) 14      b) 28      c) 51      d) 119      e) 666      f) 50 050
13. Mitkä seuraavista luvuista ovat alkulukuja?  
a) 103      b) 441      c) 733      d) 993      e) 1 237
14. Kuinka monta kertaa luku a) 30, b) 45, c) 73, d) 210 tulee poistetuksi Eratostheneen seulassa?

## 3 Syt ja pyj

### Suurin yhteinen tekijä

Annettujen luonnollisten lukujen *yhteinen tekijä* on luku, jolla kaikki annetut luvut ovat jaollisia. Yhteisistä tekijöistä suurin on nimensä mukaisesti *suurin yhteinen tekijä* (syt). (engl. *gcd, greatest common divisor*)

Luonnollisten lukujen suurin yhteinen tekijä muodostetaan niin, että luvut jaetaan ensin alkutekijöihin ja kaikki yhteiset alkutekijät kerrotaan keskenään. Tuloon otetaan alkutekijöiden pienimmät potenssit.

**Esimerkki 1**

Määritä lukujen 54, 120 ja 144 suurin yhteinen tekijä.

*Ratkaisu:*

Jaetaan luvut alkutekijöihin ja muodostetaan yhteisten tekijöiden tulo.

$$54 = 2 \cdot 27 = 2 \cdot 3 \cdot 9 = 2 \cdot 3^3$$

$$120 = 2 \cdot 60 = 2 \cdot 2 \cdot 2 \cdot 15 = 2^3 \cdot 3 \cdot 5$$

$$144 = 2 \cdot 72 = 2 \cdot 8 \cdot 9 = 2^4 \cdot 3^2$$

-----  
 $\text{syt} = 2 \cdot 3 = 6$

*Vastaus:*  $\text{syt}(54, 120, 144) = 6$

Lukuja, joiden suurin yhteinen tekijä on 1, sanotaan *keskenään jaottomiksi*. Niinpä esimerkiksi luvut 8 ja 15 ovat keskenään jaottomia, koska  $\text{syt}(8, 15) = 1$ .

**Pienin yhteinen jaettava**

Murtoluvut on ennen yhteen- ja vähennyslaskua muutettava samannimisiksi. Yhteiseksi nimittäjäksi valitaan tällöin usein nimittäjien *pienin yhteinen jaettava* (pyj). (engl. *lcm, least common multiple*)

Annettujen luonnollisten lukujen pienin yhteinen jaettava on pienin luonnollinen luku, joka on jaollinen jokaisella annetuista luvuista.

Esimerkiksi lukujen 3, 6 ja 8 pienin yhteinen jaettava  $\text{pyj}(3, 6, 8)$  on 24.

Lukujen pienin yhteinen jaettava löydetään niin, että luvut jaetaan alkutekijöihin, kutakin alkutekijää otetaan niin monta kuin sitä on siinä luvussa, jossa sitä on eniten, ja lopuksi saadut alkutekijät kerrotaan keskenään.

**Esimerkki 2**

Määritä  $\text{pyj}(42, 60, 125)$ .

*Ratkaisu:*

$$42 = 2 \cdot 3 \cdot 7$$

$$60 = 2^2 \cdot 3 \cdot 5$$

$$125 = 5^3$$

-----  
 $\text{pyj} = 2^2 \cdot 3 \cdot 5^3 \cdot 7 = 10500$

*Vastaus:*  $\text{pyj}(42, 60, 125) = 10500$

**Esimerkki 3**

Laske lausekkeen  $\frac{7}{15} + \frac{11}{45} + \frac{4}{63}$  arvo.

*Ratkaisu:*

Määritetään aluksi nimittäjien pienin yhteinen jaettava.

$$15 = 3 \cdot 5$$

$$45 = 9 \cdot 5 = 3^2 \cdot 5$$

$$63 = 9 \cdot 7 = 3^2 \cdot 7$$

-----

$$\text{pyj} = 3^2 \cdot 5 \cdot 7 = 315$$

Murtolukujen yhteiseksi nimittäjäksi valitaan  $\text{pyj}(15, 45, 63) = 315$ .

$$\frac{7}{15} + \frac{11}{45} + \frac{4}{63} = \frac{21 \cdot 7}{315} + \frac{7 \cdot 11}{315} + \frac{5 \cdot 4}{315} = \frac{244}{315} \quad \text{Vastaus: Lausekkeen arvo on } \frac{244}{315}.$$

Kahden nollasta eroavan luonnollisen luvun  $a$  ja  $b$  suurimman yhteisen tekijän ja pienimmän yhteisen jaettavan välillä on voimassa yhtälö

$$ab = \text{syt}(a, b) \cdot \text{pyj}(a, b)$$

Osoitetaan yhtälö oikeaksi. Olkoon  $\text{syt}(a, b) = c$  ja  $\text{pyj}(a, b) = d$ . Tällöin  $\text{syt}$ :n määritelmän mukaan on sellaiset keskenään jaottomat luvut  $p$  ja  $r$ , että  $a = pc$  ja  $b = rc$ . Lisäksi  $d = prc$ , joten  $ab = pc \cdot rc = c \cdot prc = cd = \text{syt}(a, b) \cdot \text{pyj}(a, b)$ .

### Tehtäviä

15. Määritä lukujen suurin yhteinen tekijä.

- a) 24 ja 66      b) 17 ja 37      c) 30, 54 ja 144      d) 8, 16, 70 ja 420

16. Supista.

- a)  $\frac{42}{63}$       b)  $\frac{121}{143}$       c)  $3\frac{33}{93}$       d)  $\frac{210}{2730}$

17. Määritä.

- a)  $\text{syt}(300, 630)$       b)  $\text{syt}(126, 792)$       c)  $\text{syt}(234, 585, 819)$       d)  $\text{syt}(105, 176, 450)$

18. Määritä lukujen pienin yhteinen jaettava.

- a) 14 ja 32      b) 14, 32 ja 36      c) 70, 240 ja 512

19. Määritä.

- a)  $\text{pyj}(15, 25, 45)$       b)  $\text{pyj}(100, 126, 315, 420)$

20. Lavenna murtoluvut samannimisiksi ja laske lausekkeen arvo.

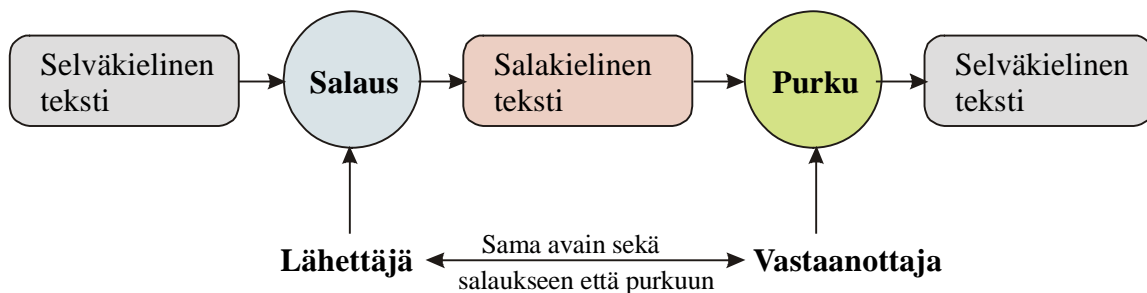
- a)  $\frac{3}{5} + \frac{1}{30} + \frac{4}{45}$       b)  $2\frac{5}{144} + \frac{7}{216}$       c)  $\frac{7}{25} + 1\frac{12}{75} - \frac{11}{105}$

21. Tiedetään, että  $\text{syt}(1\,426 \text{ ja } 1\,748) = 46$ . Määritä  $\text{pyj}(1\,426 \text{ ja } 1\,748)$ .

## 4 Salakirjoitus

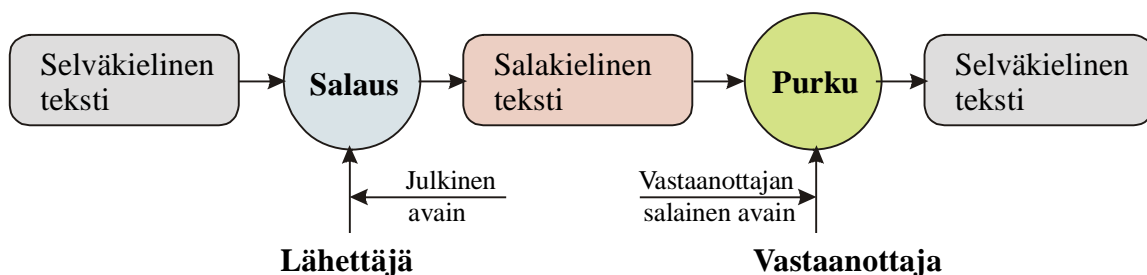
*Salakirjoitus* on menetelmä, jossa selväkielinen teksti muutetaan salakieliseksi tekstiksi. Salakirjoitustekniikoita eli *salaus algoritmeja* on monia, ja niistä yksi luotettavimmista perustuu luonnollisten lukujen jakamiseen tekijöihin. Tässä esityksessä luodaan lyhyt yleiskatsaus salakirjoituksen perinteisiin menetelmiin ja alan terminologiaan.

Salakirjoituksen *purkamisessa* teksti muutetaan takaisin selväkieliseksi tekstiksi. Tähän tarvittavaa tietoa sanotaan *avaimeksi*. Salakirjoitus ja purkaminen voidaan tehdä joko yhdellä avaimella tai kahta avainta käyttäen. Edellistä menetelmää sanotaan *symmetriseksi* ja jälkimmäistä *epäsymmetriseksi* tekniikaksi.



**Symmetrisessä salakirjoituksessa** sekä salaaminen että purkaminen tehdään samalla avaimella. Tämä yhden avaimen menetelmä on vanhin, ja siinä ongelmana on avaimen toimitaminen osapuolelta toiselle luotettavasti niin, että avain säilyy salaisena. Seuraava kaavio havainnollistaa yhden avaimen tekniikkaa.

**Epäsymmetrisessä salakirjoituksessa** eli *julkisen avaimen* tekniikassa avaimia on kaksi. *Salausavainta* käytetään tekstin salaamiseen ja *purkuavainta* salatun tekstin purkamiseen. Salausavain on julkinen, ja se voi olla vaikka kaikkien nähtävillä esimerkiksi Internetissä. Purkuavain on vastaanottajan yksityinen avain. Menetelmä toimii niin, että vastaanottaja ilmoittaa julkisesti hänelle lähetettävien viestien kirjoitusavaimen. Tätä käyttäen lähettäjä salaa viestin ja toimittaa sen vastaanottajalle, joka sitten avaa viestin hallussaan olevalla yksityisellä avaimella. Seuraava kaavio havainnollistaa julkisen avaimen tekniikkaa.



Salakirjoitusmenetelmiä on käytetty jo muinaisen Egyptin, Rooman ja Intian ajoista asti. Spartalaisten ajoista alkaen sitä on käytetty sodankäynnissä ja siihen liittyvässä tiedustelussa. Nykyisin käyttötarvetta on löytynyt paljon tietoverkkojen myötä mm. kaupankäynnissä ja tutkimuksessa. Myös yksityisillä ihmisillä on mahdollisuus salata esimerkiksi sähköpostiviestinsä.

Viestejä salakirjoitetaan, jottei niiden sisältö paljastuisi ulkopuolisille. Julkisia ja yksityisiä avaimia tuotetaan salausalgoritmeilla. Avaimen *bittisyys* tarkoittaa sitä, kuinka monesta bitistä avain muodostuu. Kolmesta bitistä saa  $2^3 = 8$  erilaista yhdistelmää ja neljästä bitistä  $2^4 = 16$  erilaista yhdistelmää, jolloin 56 tai 128 bittisillä avaimilla on jo merkitystä salauksen murta-  
misajan kannalta. Salaisen avaimen tekniikassa avaimen suositeltava minimipituus on 128 bittiä, kun taas julkisen avaimen menetelmässä avaimen pitää olla huomattavasti pitempi. Kaikesta huolimatta parhainkin salausavain voi olla murrettavissa.

## Esimerkkejä salausmenetelmistä

### Esimerkki 1

Salakirjoituksessa joka kolmas kirjain on lähetettyä tekstiä.

Helppo salausmenetelmä on sellainen, jossa esimerkiksi joka kolmas kirjain on salattavaa tekstiä. Tällöin esimerkiksi osoite PUIJONKATU voisi olla salattuna HUPASUJAITUJLIONENMYKPEAKÄTOPUUK

### Esimerkki 2

Polybiuksen salakirjoitusmenetelmä

Kreikkalainen historioitsija Polybius keksi salakirjoitusmenetelmän, jossa hän järjesti kirjaimet taulukkoon. Kirjaimia merkittiin kaksinumeroisella koodilla, jossa ensimmäinen numero ilmoittaa rivin ja toinen numero sarakkeen.

Englannin kielen aakkoset voidaan merkitä Polybiuksen mukaan neliötaulukkaan, kun kirjaimet i ja j yhdistetään samaan sarakkeeseen.

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i, j	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

Esimerkiksi kirjain b on 12 ja kirjain o 34. Sanaa "ylihuomenna" vastaa salakielisenä merkkiryhmä 5431242345343215333311.

### Esimerkki 3

Caesarin salakirjoitus

Gaius Julius Caesar salasi sotapäälliköilleen lähettämänsä viestit, että viholliset eivät saisi niitä selville. Jokainen kirjain korvattiin aakkostossa kolme kirjainta seuraavana olevalla kirjaimella. Aakkoston lopusta siirrytään korvausmenettelyssä alkuun. Menetelmässä esimerkiksi kirjain a korvataan kirjaimella d ja kirjain z kirjaimella c. Salauksia, joissa korvaus voi alkaa muullakin kirjaimella kuin kirjaimella d, kutsutaan myös Caesarin salakirjoitukseksi.

Esimerkiksi teksti Veni, vidi, vici olisi salattuna yhql , ylgl , ylfl.

Caesarin salakirjoitus ja sen muunnokset on murrettavissa kokeilemalla vaikka kaikki 26 siirrosta englannin kielen aakkosissa tai vaikka kaikki 29 siirrosta suomen kielen aakkosissa.

**Esimerkki 4**

One time pad

One time pad on salaus, joka oikein toteutettuna on murttamaton. Avain on aina yhtä pitkä kuin salattava teksti. Samaa avainta ei koskaan saa käyttää kahta kertaa ja avaimen on oltava aina satunnainen. Tavalliseen salauskäyttöön one time pad ei ole kelvöllinen.

**Esimerkki 5**

RSA-salankirjoitus

Rivestin, Shamirin ja Adlemanin vuonna 1977 kehittämä menetelmä on yksi käytetyimpiä julkisen avaimen tekniikoita. Se perustuu siihen, että suurten kokonaislukujen jakaminen alkutekijöihin on vaikea tehtävä, kun taas suurien alkulukujen on helppo löytää. Julkisenä kirjoitusavaimena on kahden suuren alkuluvun tulo. Salainen lukuavain edellyttää näiden alkulukujen tuntemista. Kun valitaan kyllin suuret alkuluvut, salaisen avaimen selvittäminen parhaillakin tietokoneohjelmilla voi viedä vuosikausia.

**Esimerkki 6**

Sähköpostiviestin salaus

Sähköpostin salaus perustuu epäsymmetriseen salankirjoitukseen. Sekä sähköpostiviestin lähettäjä että vastaanottaja luovat itselleen avainparin sähköpostiohjelmaan asennetulla salausohjelmalla. Molemmat pitävät salassa yksityisen avaimensa, mutta antavat toisilleen julkisen avaimen.

Jos nyt esimerkiksi Kalle lähettää viestin Iidalle, niin hän salaa sen Iidan julkisella avaimella, ja Iida voi purkaa sen yksityisellä avaimellaan. Toisin päin lähetettynä Iida salaa viestin Kallen julkisella avaimella, ja Kalle purkaa sen yksityisellä avaimellaan.

**Esimerkki 7**

Puhuttu salakieli

Yhdysvallat käytti toisen maailmansodan aikana navajointiaaneja viestintätehtävissä. He käyttivät omaa äidinkieltään lähettäessään viestejä radiolla. Navajon kieltä ei tuolloin vielä tunnettu Yhdysvaltojen ulkopuolella, joten japanilaiset ja saksalaiset eivät ymmärtäneet viestien sisältöä. Toisen maailmansodan aikaisille aseille ei navajon kielessä ollut vastinetta, joten niille annettiin peitenimet.

**Tehtäviä**

22. Salaa oma postiosoitteesi esimerkin 1 menetelmällä niin, että joka neljäs kirjain tai numero on osoitteesi tekstiä.
23. Salaa Polybiuksen salankirjoitusmenetelmällä seuraava teksti: Kryptografia on tiede, joka tutkii, miten tekstejä voidaan salata ulkopuolisilta.
24. Salaa Caesarin menetelmällä seuraava teksti: Kryptoanalyysi tutkii, kuinka salattuja viestejä voidaan purkaa tietämättä avainta. Korvaa jokainen kirjain suomalaisten aakkosten neljä kirjainta seuraavana olevalla kirjaimella.

25. *Atbash*-salakirjoitus on yksi vanhimmista salakirjoitusmenetelmistä, josta on esimerkkejä jo Raamatussa. Kysymyksessä on korvausmenetelmä, joka vain kääntää aakkoston eli suomalaisessa aakkostossa salaa kirjaimen A kirjaimeksi Ö, kirjaimen B kirjaimeksi Ä jne.  
Salaa *Atbash*menetelmällä seuraava teksti: Kryptologia on matemaattinen tiede, joka tutkii salakirjoitusta. Kryptografia ja kryptoanalyysi ovat sen osa-alueita.

## Vastauksia ja ratkaisuehdotuksia

- Väite ei pidä paikkaansa, sillä luvun 1 503 viimeinen numero ei ole 0, 2, 4, 6 tai 8.
  - Väite pitää paikkansa, sillä luku 1 565 ei ole jaollinen kuudella.
  - Väite pitää paikkansa, sillä luku 72 000 päättyy nolllaan.
  - Väite pitää paikkansa. Luku 4 214 voidaan kirjoittaa summana  $4\,200 + 14$ , josta seitsemällä jaollisuuden näkee helposti.
- Luvulla 1 000 on viisitoista erisuurta tekijää: 1, 2, 4, 8, 10, 20, 25, 40, 50, 100, 125, 200, 250, 500 ja 1 000.
- Luku 434 ei ole jaollinen luvulla 4, sillä luku 34 ei ole jaollinen neljällä.
  - Luku 2 444 on jaollinen luvulla 4, sillä luku 44 on jaollinen neljällä.
  - Luku 11 036 on jaollinen luvulla 4, sillä luku 36 on jaollinen neljällä.
  - Luku 630 254 ei ole jaollinen luvulla 4, sillä luku 54 ei ole jaollinen neljällä.
- Luku 787 ei ole jaollinen luvulla 7, sillä luku  $78 - 2 \cdot 7 = 64$  ei ole jaollinen seitsemällä.
  - Luku 1 001 on jaollinen luvulla 7, sillä luku  $100 - 2 \cdot 1 = 98$  on jaollinen seitsemällä.
  - Luku 3 300 ei ole jaollinen luvulla 7. Perustelut:  $330 - 2 \cdot 0 = 330$ , edelleen  $33 - 2 \cdot 0 = 33$ , josta nähdään seitsemällä jaottomuus.
  - Luku 332 640 on jaollinen luvulla 7. Perustelut:  $33\,264 - 2 \cdot 0 = 33\,264$ , edelleen  $3\,326 - 2 \cdot 4 = 3\,318$ ,  $331 - 2 \cdot 8 = 315$ ,  $31 - 2 \cdot 5 = 21$ . Viimeksi saadusta luvusta selviää seitsemällä jaollisuus.
- Luku 11 111 ei ole jaollinen luvulla yksitoista. Perustelut: parittomien numeromerkkien summa on 3 ( $= 1 + 1 + 1$ ) ja parillisten numeromerkkien summa on 2 ( $= 1 + 1$ ). Saatujen summien erotus 1 ei ole jaollinen luvulla 11.
  - Luku 271 590 on jaollinen luvulla yksitoista. Perustelut:  $2 + 1 + 9 = 12$ , vastaavasti  $7 + 5 + 0 = 12$ . Koska saatujen summien erotus on 0, annettu luku on jaollinen luvulla yksitoista.
  - Luku 72 011 ei ole jaollinen luvulla 11. Perustelut:  $7 + 0 + 1 = 8$ , vastaavasti  $2 + 1 = 3$ . Summien erotus 5 ei ole jaollinen luvulla yksitoista.
  - Luku 171 028 on jaollinen luvulla yksitoista. Perustelut:  $1 + 1 + 2 = 4$  ja vastaavasti  $7 + 0 + 8 = 15$ . Summien erotus  $4 - 15 = -11$  on jaollinen luvulla yksitoista.

6. a) Luku on jaollinen 2:lla, koska viimeinen numero on 6.  
 b) Luku on jaollinen 3:lla, koska numeroiden summa 54 on jaollinen kolmella ( $54 = 3 \cdot 18$ )  
 c) Luku on jaollinen 4:llä, koska luku 36 on jaollinen neljällä.  
 d) Luku ei ole jaollinen 5:llä, koska viimeinen numero ei ole 0 eikä 5.  
 e) Luku on jaollinen 6:lla, sillä edellisen perusteella luku on jaollinen sekä 2:lla että 3:lla.  
 f) Luku ei ole jaollinen 7:llä. Perustelut:  $2\ 345\ 789\ 013 - 2 \cdot 6 = 2\ 345\ 789\ 001$   
 $2\ 345\ 678\ 900 - 2 \cdot 1 = 2\ 345\ 678\ 898$ ,  $234\ 567\ 889 - 2 \cdot 8 = 234\ 567\ 873$   
 $23\ 456\ 787 - 2 \cdot 3 = 23\ 456\ 781$   $2\ 345\ 678 - 2 \cdot 1 = 2\ 345\ 676$   
 $234\ 567 - 2 \cdot 6 = 234\ 555$   $23\ 455 - 2 \cdot 5 = 23\ 445$   
 $2\ 344 - 2 \cdot 5 = 2\ 334$   $233 - 2 \cdot 4 = 225$   
 $22 - 2 \cdot 5 = 12$   
 g) Luku on jaollinen 8:lla, sillä kolmen viimeisen numeron muodostama luku 136 on jaollinen kahdeksalla ( $136 = 8 \cdot 17$ ).  
 h) Luku on jaollinen 9:llä, sillä numeroiden summa 54 on jaollinen yhdeksällä ( $54 = 9 \cdot 6$ )  
 i) Luku ei ole jaollinen 10:llä, sillä luvun viimeinen numero ei ole 0.  
 j) Luku ei ole jaollinen 11:llä, sillä parittomien numeromerkkien summa on 23, ja parillisten summa 31, jolloin erotus on  $-8$ .
7. Olkoon tulon  $ab$  tekijä  $a$  jaollinen luvulla  $c$ . Silloin on olemassa sellainen luku  $k$ , että  $a = kc$ . Tällöin  $ab = kcb = c \cdot kb$ . Tulos merkitsee, että  $c \mid ab$ .
8. Kyseiset luvut ovat luvun 77 kolminumeroisia monikertoja: 154, 231, 308, 385, 462, 539, 616, 693, 770, 847 ja 924.
9. a) Luku 491 049 ei ole jaollinen seitsemällä. Kirjoitetaan luku summana.  $491\ 049 = 491\ 000 + 49$ . Summan jälkimmäinen yhteenlaskettava on jaollinen seitsemällä, mutta edellinen yhteenlaskettava ei ole.  
 b) Luku 99 011 on jaollinen yhdellätoista. Kirjoitetaan luku summana  $99\ 011 = 99\ 000 + 11$ . Molemmat yhteenlaskettavat ovat jaollisia yhdellätoista ( $99\ 000 = 9 \cdot 11\ 000$ )
10. Katso kansikuva. Kysytyjä alkulukuja ovat 2, 3, 5, 7, 11, 13, 17, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 ja 97.
11. Vain yksi eli luku 2.
12. a)  $14 = 2 \cdot 7$       b)  $28 = 2^2 \cdot 7$       c)  $51 = 3 \cdot 17$       d)  $119 = 7 \cdot 17$   
 e)  $666 = 2 \cdot 3^2 \cdot 37$       f)  $50\ 050 = 2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$
13. Alkulukuja ovat luvut 103, 733 ja 1 237.
14. a) kolme kertaa      b) kaksi kertaa      c) ei kertaakaan      d) neljä kertaa

15. a)

$$\begin{array}{l} 24 = 2^3 \cdot 3 \\ 66 = 2 \cdot 3 \cdot 11 \\ \hline \text{syt} = 2 \cdot 3 = 6 \end{array}$$

b)

$$\begin{array}{l} 17 = 1 \cdot 17 \\ 37 = 1 \cdot 37 \\ \hline \text{syt} = 1 \end{array}$$

c)

$$\begin{array}{l} 30 = 2 \cdot 3 \cdot 5 \\ 54 = 2 \cdot 3^3 \\ 144 = 2^4 \cdot 3^2 \\ \hline \text{syt} = 2 \cdot 3 = 6 \end{array}$$

d)

$$\begin{array}{l} 8 = 2^3 \\ 16 = 2^4 \\ 70 = 2 \cdot 5 \cdot 7 \\ 420 = 2^2 \cdot 3 \cdot 5 \cdot 7 \\ \hline \text{syt} = 2 \end{array}$$

16. a)  $\frac{42}{63} = \frac{2 \cdot 3 \cdot 7}{3 \cdot 3 \cdot 7} = \frac{2}{3}$

b)  $\frac{121}{143} = \frac{11 \cdot 11}{11 \cdot 13} = \frac{11}{13}$

c)  $3 \frac{33}{93} = 3 \frac{3 \cdot 11}{3 \cdot 31} = 3 \frac{11}{31}$

d)  $\frac{210}{2730} = \frac{10 \cdot 3 \cdot 7}{10 \cdot 3 \cdot 7 \cdot 13} = \frac{1}{13}$

17. a)  $\begin{array}{l} 300 = 2^2 \cdot 3 \cdot 5^2 \\ 630 = 2 \cdot 3^2 \cdot 5 \cdot 7 \\ \hline \text{syt} = 2 \cdot 3 \cdot 5 = 30 \end{array}$

b)  $\begin{array}{l} 126 = 2 \cdot 3^2 \cdot 7 \\ 792 = 2^3 \cdot 3^2 \cdot 11 \\ \hline \text{syt} = 2 \cdot 3^2 = 18 \end{array}$

c)  $\begin{array}{l} 234 = 2 \cdot 3^2 \cdot 13 \\ 585 = 3^2 \cdot 5 \cdot 13 \\ 819 = 3^2 \cdot 7 \cdot 13 \\ \hline \text{syt} = 3^2 \cdot 13 = 117 \end{array}$

d)  $\begin{array}{l} 105 = 3 \cdot 5 \cdot 7 \\ 176 = 2^4 \cdot 11 \\ 450 = 2 \cdot 3^2 \cdot 5^2 \\ \hline \text{syt} = 1 \end{array}$

18. a)  $\begin{array}{l} 14 = 2 \cdot 7 \\ 32 = 2^5 \\ \hline \text{pyj} = 2^5 \cdot 7 = 224 \end{array}$

b)  $\begin{array}{l} 14 = 2 \cdot 7 \\ 32 = 2^5 \\ 36 = 2^2 \cdot 3^2 \\ \hline \text{pyj} = 2^5 \cdot 3^2 \cdot 7 = 2\,016 \end{array}$

c)  $\begin{array}{l} 70 = 2 \cdot 5 \cdot 7 \\ 240 = 2^4 \cdot 3 \cdot 5 \\ 512 = 2^9 \\ \hline \text{pyj} = 2^9 \cdot 3 \cdot 5 \cdot 7 = 53\,760 \end{array}$

19. a)  $\begin{array}{l} 15 = 3 \cdot 5 \\ 25 = 5^2 \\ 45 = 3^2 \cdot 5 \\ \hline \text{pyj} = 3^2 \cdot 5^2 = 225 \end{array}$

b)  $\begin{array}{l} 100 = 2^2 \cdot 5^2 \\ 126 = 2 \cdot 3^2 \cdot 7 \\ 315 = 3^2 \cdot 5 \cdot 7 \\ 420 = 2^2 \cdot 3 \cdot 5 \cdot 7 \\ \hline \text{pyj} = 2^2 \cdot 3^2 \cdot 5^2 \cdot 7 = 6\,300 \end{array}$

20. a)  $\frac{18)}{5} + \frac{3)}{30} + \frac{2)}{45} = \frac{54}{90} + \frac{3}{90} + \frac{8}{90} = \frac{65}{90} = \frac{13}{18}$

b)  $2 \frac{3)}{144} + \frac{2)}{216} = 2 \frac{15}{432} + \frac{14}{432} = 2 \frac{29}{432}$

$$c) \quad \frac{7}{25} + 1\frac{12}{75} - \frac{11}{105} = \frac{147}{525} + 1\frac{84}{525} - \frac{55}{525} = 1\frac{176}{525}$$

21. Käytetään hyväksi tietoa, että  $\text{sy}(a, b) \cdot \text{pyj}(a, b) = ab$ . Tällöin

$$46 \cdot \text{pyj}(1\,426 \text{ ja } 1\,748) = 1\,426 \cdot 1\,748,$$

josta edelleen  $\text{pyj}(1\,426 \text{ ja } 1\,748) = 54\,188$ .

23. 254254354434224211212411 3433 4424151415, 24342511 444544252424,  
3224441533 4415254344152411 51342414111133 431131114411  
4531253435453431244324314411.

24. Ovötxserepööwm xyxomm, oymroe wepexxyne zmiwxinc zsmheer tyvoee xmixcqcxxc  
dzdmrxe.

25. Slenjorowuö op qöjyqööjjupyp juyzy, tosö jijsuu körösultoujikjö. Slenjowlöxuö tö slen-  
joöpöreeku ohöj kyp okööriyujö.

Alla olevasta taulukosta löytyvät helposti Atbash-koodin käyttämät vastinkirjaimet.  
Koodi on hyvin helppo murtaa eikä sitä vaikeuta juurikaan tekstin kirjoittaminen ilman  
tavanomaisia sana- tai virkevälejä: slenjorowuöopqöjyqööjjupypjuyzytosöjijisuukö  
rösultoujikjöslenjowlöxuötöslenjoöpöreekuohöjkypokööriyujö

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	Å	Ä	Ö
Ö	Ä	Å	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

## Aiheeseen liittyviä poimintoja

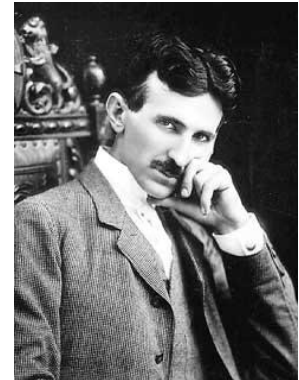
### Luonnolliset luvut

Matemaattisessa kirjallisuudessa esiintyy kaksi tulkintaa luonnollisten lukujen joukolle  $\mathbb{N}$ . Joskus sillä tarkoitetaan joukkoa  $\{1, 2, 3, \dots\}$  mutta nykyisin hyvin yleisesti myös joukkoa  $\{0, 1, 2, 3, \dots\}$ . Kysymys on sopimuksesta, ja määrittely riippuu usein kirjoittajan omasta tottumuksesta.

Luku 0 ei ollut lainkaan mukana varhaisimmissa lukujen järjestelmissä, joissa luvut olivat vahvasti sidoksissa lukumääriin. Nolla saatettiin tuntea, mutta sitä pidettiin hyödyttömänä. Esimerkiksi Aristoteleen mukaan nolla jotakin ei ole mitään jostakin. Nykyiset numeromerkit 1, 2, 3, ..., 9 pohjautuvat varhaisiin hinduilta peräisin oleviin kirjoituksiin ja Espanjan maurien arabialaisiin numeroihin. Joskus numeromerkkien loppuun kirjoitettiin viimeiseksi pyöreä täplä nollan merkiksi. Sen tärkeyden ilmaisivat arabialaiset eräässä matematiikan historian sattuvassa lauseessa: "Kun (vähennyslaskussa) mitään ei jää jäljelle, kirjoita pieni ympyrä, ettei paikka jää tyhjäksi". (Lähde: Lukujen maailma, Life-tietokirjat 1972)

### Tesla ja kolmonen

Nikolai Tesla (1856–1943) oli nykyisen Kroatian alueella syntynyt ja vuonna 1884 Yhdysvaltoihin muuttanut nerokas fyysikko, jota pidetään yhtenä nykyajan suurimmista keksijöistä. Hän kehitti ns. teslamuuntajan, keksi siirtää sähköenergiaa vaihtovirtaa käyttäen ja kehitti loisteputken idean. Hän keksi oikosulkumoottorin, joka on erittäin kestävä ja teollisuudessa yleisimmin käytetty vaihtovirtamoottorityyppi. Myös radioaalloilla toimivat kauko-ohjain on yksi lukuista Teslan keksinnöistä.



Teslalle luku 3 ja kolmella jaollisuus oli tärkeä. Leipä piti leikata 9 viipaleeksi, astioita ja pyyhkeitä piti olla 3 tai 9, ja hotellihuoneessa asuessaan hän pyysi aina 9 nenäliinaa. Hotellihuoneeksi, jossa hän asui kymmenkunta vuotta, hän vaati saada huoneen 3327, koska tuo luku on kolmella jaollinen.

Pakkomielteistä huolimatta Teslan nerous on kiistämätöntä. Hänen mukaansa on nimetty magneettivuon tiheyden  $B$  yksikkö  $1 \text{ T} = \text{tesla}$ .

### Suurin tunnettu alkuluku

Jo Eukleides (noin 300 eaa) todisti, että alkulukuja on äärettömän monta. Suurinta alkulukua ei siis ole, mutta aina vain suurempia haetaan jopa kilpailumielessä. Tällä hetkellä (toukokuu 2009) suurin tunnettu alkuluku on  $2^{43112} \cdot 609 - 1$ . Siinä on lähes 13 miljoonaa numeroa, ja se tuotti löytäjilleen 100 000 dollarin palkinnon. Luvun auki kirjoittamiseen tarvittaisiin yli kolme tuhatta A4-kokoa olevaa tekstisivua. Niistä tulisi noin 15 cm paksu kirja.