Lukuteorian alkeita

Matematiikkakilpailuissa on yleensä tehtäviä, joiden aiheala on alkeellinen lukuteoria. Tässä esitellään perustellen ne lukuteorian tiedot, joihin lukuteoria-aiheisissa tehtävissä yleensä viitataan. Kuten huomataan, "kilpailulukuteoria" sisältää jonkin verran ainesta, joka ei kuulu lukion lukuteoria ja logiikka -nimiseen kurssiin.

Lukuteoriassa käytetään hyväksi eräitä yleisiä lähinnä joukko-opillisia luonnollisten lukujen joukon ominaisuuksia. Tässä esityksessa vedotaan ainakin *induktioperiaatteeseen* ja sen kanssa yhtäpitävään tulokseen, jonka mukaan alhaalta rajoitetussa kokonaislukujoukossa on pienin luku ja ylhäältä rajoitetussa kokonaislukujoukossa on suurin luku.

1. Jaollisuus. Lukuteoriassa tarkastellaan yleensä *luonnollisia lukuja*[1] 1, 2, 3, ... ja *kokonaislukuja* ..., −2, −1, 0, 1, 2, ... Kokonaisluku q on *jaollinen* kokonaisluvulla p, merkittynä $p|q$, jos on olemassa kokonaisluku n siten, että $q = np$. Tällöin sanotaan myös, että p on q:n *tekijä* tai että p *jakaa* q*:n*.

2. Suurin yhteinen tekijä. Kokonaislukujen a ja b *suurin yhteinen tekijä* d on se (yksikäsitteinen) luonnollinen luku d, jolle pätee $d|a$ ja $d|b$ sekä jos $c|a$ ja $c|b$, niin $c \leq d$. Merkitään $d = \text{s.y.t.}(a, b) = (a, b)$. (Englanninkielisessä tekstissä suurin yhteinen tekijä on GCD, *greatest common divisor*.) Selvästi aina $1 \leq (a, b) \leq \min\{|a|, |b|\}$.

Lause. *Jos* $(a, b) = d$, *niin* $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Todistus. Merkitään $c = \left(\frac{a}{d}, \frac{b}{d}\right)$. Silloin $1 \leq c$. Toisaalta, koska c on lukujen $\frac{a}{d}$ ja $\frac{b}{d}$ tekijä, on olemassa luonnolliset luvut m ja n siten, että $\frac{a}{d} = mc$, $\frac{b}{d} = nc$ eli $a = m(cd)$, $b = n(cd)$. Siis cd on sekä a:n että b:n tekijä, joten $cd \leq d$. Siis $c \leq 1$. □

Useamman kuin kahden luvun $a_1, a_2, \ldots, a_n$ suurin yhteinen tekijä

$$(a_1, a_2, \ldots, a_n)$$

määritellään palautuskaavan

$$(a_1, a_2, \ldots, a_n) = ((a_1, a_2, \ldots, a_{n-1}), a_n)$$

avulla. Useamman kuin kahden luvun suurimman yhteisen tekijän ominaisuudet ovat analogisia kahden luvun surimman yhteisen tekijän minaisuuksien kanssa.

3. Jakoyhtälö. *Kaikilla kokonaisluvuilla* a *ja* b, $b > 0$, *on olemassa sellaiset kokonaisluvut* q *ja* r, *missä* $0 \leq r < b$, *että*

$$a = qb + r.$$

Todistus. Olkoon r_0 pienin ei-negatiivinen luku, joka on muotoa $a - qb$, missä q on kokonaisluku. Oletetaan, että $r_0 > b$. Mutta silloin olisi myös $a - (q + 1)b = r_0 - b > 0$, vastoin r_0:sta tehtyä oletusta. □

[1] Toisinaan myös lukua 0 pidetään luonnollisena lukuna.

Lause. *Jos* $a = qb + r$, *niin* $(a,\, b) = (b,\, r)$.

Todistus. Luku $(a,\, b)$ on b:n tekijä. Koska (a, b) on a:n ja b:n tekijä, se on myös r:n tekijä. Siis $(a, b) \leq (b, r)$. Täsmälleen samoin päätellään, että $(b, r) \leq (a, b)$. □

4. Eukleideen algoritmi. Olkoon $b > 0$. Jakoyhtälöä ja sitä seurannutta lausetta toistuvasti käyttämällä voidaan aina määrittää a:n ja b:n suurin yhteinen tekijä (a, b): On olemassa q_1 ja $r_1 < b$ siten, että $a = q_1 b + r_1$. Jos $r_1 > 0$, on olemassa q_2 ja $r_2 < r_1$ siten, että $b = q_2 r_1 + r_2$. Jatkamalla näin saadaan jonot lukuja q_k, r_k, missä aina $r_{k-2} = q_k r_{k-1} + r_k$ ja $r_1 > r_2 > \ldots > r_k > \ldots \geq 0$. Jollakin indeksin k arvolla on silloin varmasti $r_{k-1} > 0$, $r_k = 0$. Kohdan 3 tuloksen perusteella on nyt $(r_{k-2},\, r_{k-1}) = (r_{k-3}, r_{k-2}) = \ldots = (b, r_1) = (a, b)$. Lisäksi (jakoyhtälö!) $(r_{k-2},\, r_{k-1}) = r_{k-1}$, joten $(a,\, b)$ on edelliseen prosessiin sisältyvän jakoketjun viimeinen nollasta eroava jakojäännös.

5. Diofantoksen yhtälön $ax+by = d$ **(eräs) ratkaisu.** Jos a, b ja d ovat kokonaislukuja, niin tehtävää, jossa on määritettävä ehdon

$$ax + by = d$$

toteuttavat *kokonaisluvut* x ja y, sanotaan *ensimmäisen asteen Diofantoksen yhtälöksi*. Oletetaan, että $d = (a, b)$. Tehtävä saadaan ratkaistuksi, kun luetaan Eukleideen algoritmissa esiintyvät jakoyhtälöt lopusta alkuun:

$$\begin{aligned} d = r_{k-1} &= r_{k-3} - q_{k-1} r_{k-2} = r_{k-3} - (r_{k-4} - q_{k-2} r_{k-3}) q_{k-1} \\ &= (1 + q_{k-1} q_{k-2}) r_{k-2} - q_{k-2} r_k r_{k-3} = \ldots = (\text{ kok.luku })a + (\text{ kok.luku })b \\ &= ax + by. \end{aligned}$$

Jos $(a,\, b) = 1$, sanotaan, että a ja b ovat *yhteistekijättömiä* tai *suhteellisia alkulukuja.*

Lause. *Jos* $(d,\, a) = 1$ *ja* $d|ab$, *niin* $d|b$.

Todistus. Edellä sanotun perusteella on olemassa sellaiset kokonaisluvut x ja y, että $dx + ay = 1$. Siis $(db)x + (ab)y = b$. Luku d on tekijänä molemmissa vasemman puolen yhteenlaskettavissa, joten se on tekijänä myös oikealla puolella eli luvussa b. □

Induktiolla voidaan edelleen todistaa, että jos $n = a_1 a_2 \cdots a_k b$, $(d,\, a_i) = 1$, kun $i = 1, \ldots, k$ ja $d \mid n$, niin $d \mid b$. – Tämän asian voi ilmaista myös niin, että jos luku on yhdistetyn luvun tekijä, se on jonkin tämän luvun tekijän tekijä.

Lause. *Jos* $(a, b) = d$ *ja* $c|a$, $c|b$, *niin* $c|d$.

Todistus. Väite seuraa yhtälön $ax + by = d$ toteuttavien lukujen x ja y olemassaolosta ja siitä, että $c|(ax + by)$. □

6. Alkuluvut. Positiivinen luku $p > 1$ on *alkuluku,* jos siitä, että $c|p$ seuraa, että $|c| = p$ tai $|c| = 1$. Positiivinen luku $q > 1$, joka ei ole alkuluku, on *yhdistetty luku*. Yhdistetyllä luvulla on muita tekijöitä kuin se itse tai 1. Huomattakoon, että luku 1 ei ole alkuluku eikä yhdistetty luku.

Lause. *Jokainen kokonaisluku* $n > 1$ *on jaollinen jollakin alkuluvulla.*

Todistus. Induktiotodistus: 2 on alkuluku ja siis jaollinen alkuluvulla. Induktio-oletus: jokainen $k \leq n$ on jaollinen alkuluvulla. Luku $n + 1$ on joko alkuluku tai yhdistetty luku. Jos se on yhdistetty luku, on $n + 1 = pq$, missä $p \leq n$. Oletuksen nojalla p on jaollinen alkuluvulla, joten niin on myös $n + 1$. □

Lause. *Jokainen kokonaisluku $n > 1$ on alkuluku tai alkulukujen tulo.*

Todistus. Induktiotodistus. Luku 2 on alkuluku. Jos jokainen $k \leq n$ on alkuluku tai alkulukujen tulo ja $n+1$ ei ole alkuluku, niin $n+1 = pq$, missä p ja q ovat alkulukuja tai alkulukujen tuloja. □

Luvun alkutekijöiden etsimistä helpottaa seuraava tulos.

Lause. *Jos n on yhdistetty luku, niin sillä on tekijä, joka on $\leq \sqrt{n}$.*

Todistus. $n = pq$, missä $1 < p < n$ ja $1 < q < n$. Jos sekä p että q olisivat $> \sqrt{n}$, jouduttaisiin ristiriitaan $pq > n$. □

Seuraavaa tulosta kutsutaan *aritmetiikan peruslauseeksi.*

Lause. *Kokonaisluvun esitys alkulukujen tulona on yksikäsitteinen, lukuun ottamatta tekijöiden järjestystä.*

Todistus. Riittää, kun tarkastellaan tapausta, jossa kokonaisluku n on yhdistetty. Olkoon $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$, missä $p_1, \ldots, p_k, q_1, \ldots, q_l$ ovat alkulukuja ja $k \leq l$. Koska p_1 on luvun $q_1 \cdots q_l$ tekijä, se on jonkin q_j:n tekijä (kohdassa 5 todistettua). Voidaan olettaa, että p_1 on q_1:n tekijä. Koska q_1 on alkuluku ja $p_1 > 1$, on oltava $p_1 = q_1$. Siis $p_2 \cdots p_k = q_2 \cdots q_l$. Edellinen päättely voidaan toistaa k kertaa. Jos $k = l$, on saatu haettu yksikäsitteisyys. Jos $k < l$, päädytään mahdottomaan yhtälöön $1 = q_{k+1} \cdots q_l$. □

Tuloesityksen perusteella saadaan uusi keino lukujen m ja n suurimman yhteisen tekijän (m, n) laskemiseksi: jos

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}, \tag{1}$$

ja

$$n = p_1^{\beta_1} p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}, \tag{2}$$

p_i:t ovat eri alkulukuja ja $\alpha_i \geq 0$ ja $\beta_i \geq 0$ kaikilla $i = 1, 2, \ldots, k$, niin

$$(m, n) = p_1^{\gamma_1} p_2^{\gamma_2} \cdot \ldots \cdot p_k^{\gamma_k},$$

missä $\gamma_i = \min\{\alpha_i, \beta_i\}$.

7. Pienin yhteinen monikerta. Lukujen m ja n *pienin yhteinen monikerta* (eli *pienin yhteinen jaettava*) p.y.m.(m, n) on positiivinen luku a, jolle on voimassa $m|a$ ja $n|a$, ja jos b on positiivinen ja $m|b$, $n|b$, niin $a \leq b$. (Englanninkielisissä teksteissä pienin yhteinen monikerta on LCD, *least common denominator*.)

Merkitään $a = \text{p.y.m.}(m, n) = [m, n]$. Jos m ja n ovat kuten kaavoissa (1) ja (2), niin

$$[m, n] = p_1^{\delta_1} p_2^{\delta_2} \cdot \ldots \cdot p_k^{\delta_k},$$

missä $\delta_i = \max\{\alpha_i, \beta_i\}$. (Miksi?) Koska $\gamma_i + \delta_i = \alpha_i + \beta_i$, on

$$(m, n)[m, n] = mn.$$

8. Alkulukujen määrä.

Lause. *Alkulukuja on äärettömän paljon.*

Todistus. Tehdään vastaoletus: alkulukujen joukko on äärellinen joukko

$$\{p_1, p_2, \ldots, p_k\}.$$

Olkoon $n = p_1 p_2 \cdot \ldots \cdot p_k + 1$. Kohdan 6 lauseen perusteella luvulla n on alkutekijä p, joka on eräs luvuista p_i, $i = 1, 2, \ldots, k$. Koska $p|n$ ja p on tekijänä myös luvussa $p_1 p_2 \cdot \ldots \cdot p_k$, joudutaan ristiriitaan $p|1$. □

Kaikki alkuluvut voi tuottaa ns. *Eratostheneen seulalla*: kirjoitetaan kaikki luonnolliset luvut jonoon, pyyhitään ensin pois kahdella jaolliset 4, 6, 8, ..., sitten kolmella jaolliset (6), 9, (12), 15,..., sitten viidellä jaolliset (10), (15), (20), 25, (30), 35, ...jne. Jäljelle jäävät alkuluvut ja vain ne.

9. Lineaaristen Diofantoksen yhtälöiden ratkaisut.

Lause. *Yhtälöllä*

$$ax + by = c$$

on kokonaislukuratkaisu x, y silloin ja vain silloin, kun $(a, b)|c$.

Todistus. Jos yhtälöllä on ratkaisu, niin $(a, b)|c$. Oletetaan, että $(a, b)|c$ ja merkitään $(a, b) = d$. Silloin $c = md$, missä m on kokonaisluku. Yhtälöllä $ax + by = d$ on kohdan 5 mukaan ratkaisu x', y'. Selvästi $x = mx'$, $y = my'$ on alkuperäisen yhtälön ratkaisu. □

Tarkastellaan vielä Diofantoksen yhtälöä $ax + by = c$, missä $\dfrac{c}{(a, b)}$ on kokonaisluku (ja yhtälöllä on siis ratkaisu). Olkoon $a' = \dfrac{a}{(a, b)}$, $b' = \dfrac{b}{(a, b)}$ ja $c' = \dfrac{c}{(a, b)}$. Tällöin yhtälöt $ax + by = c$ ja $a'x + b'y = c'$ ovat yhtäpitävät, joten niillä on samat ratkaisut. Koska $(a', b') = 1$ (kohta 2), voidaan rajoittua tutkimaan sellaisia yhtälöitä $ax + by = c$, joissa $(a, b) = 1$.

Lause. *Olkoon $(a, b) = 1$, $ab \neq 0$ ja $ax_0 + by_0 = c$. Silloin yhtälön $ax + by = c$ kaikki ratkaisut ovat*

$$x = x_0 + bt, \quad y = y_0 - at,$$

missä t saa kaikki kokonaislukuarvot.

Todistus. Olkoon t mielivaltainen kokonaisluku. Silloin

$$a(x_0 + bt) + b(y_0 - at) = ax_0 + by_0 = c.$$

Jos toisaalta $ax+by = c$, niin $a(x-x_0)+b(y-y_0) = 0$. Siis $b|(a(x-x_0))$, ja koska $(a, b) = 1$, niin $b|(x-x_0)$. Siis $x-x_0 = bt$ jollakin kokonaisluvulla t. Samoin nähdään, että $y-y_0 = at'$ jollakin kokonaisluvulla t'. Mutta koska $0 = ax+by-c = ax_0+abt+by_0+bat'-c = ab(t+t')$ ja $ab \neq 0$, on $t = -t'$. □

10. Kongruenssit. Olkoon c positiivinen kokonaisluku. Lukujen a ja b sanotaan olevan *kongruentteja modulo c*, jos $c|(b - a)$ eli jos $a = b + kc$ jollakin kokonaisluvulla k. Tällöin merkitään $a \equiv b \mod c$ (tai jos epäselvyyden vaaraa ei ole, vain $a \equiv b$). Relaatiota $a \equiv b \mod c$ sanotaan *kongruenssiksi*.

Jos a on mielivaltainen kokonaisluku ja c on positiivinen kokonaisluku, on aina olemassa ehdon $0 \leq r < c$ täyttävä luku r siten, että $a \equiv r \mod c$. Tämä seuraa jakoyhtälöstä.

Kongruenssit ovat erittäin käyttökelpoisia jaollisuuteen liittyvissä tehtävissä. Tämä perustuu siihen, että kongruenssi käyttäytyy tavallisten laskutoimitusten suhteen lähes samoin kuin tavallinen lukujen yhtäsuuruus.

Oletetaan, että $a \equiv b \bmod m$ ja $c \equiv d \bmod m$. Silloin on voimassa

$$a + c \equiv b + d \bmod m$$
$$ac \equiv bd \bmod m$$

ja

$$a^k \equiv b^k \bmod m$$

kaikilla positiivisilla kokonaisluvuilla k.

Todistetaan esimerkiksi keskimmäinen relaatio: Oletuksesta seuraa, että $a = b + em$ ja $c = d + fm$, missä e ja f ovat kokonaislukuja. Siis

$$ac = (b + em)(d + fm) = bd + (efm + bf + ed)m = bd + gm,$$

missä g on kokonaisluku.

Jakolaskun suhteen kongruensseille pätee seuraavaa: jos $ac \equiv bc \bmod m$ ja $(c,\, m) = 1$, niin $a \equiv b \bmod m$.

Todistus: Olkoon $ac - bc = km$. Koska $(a - b)c$ on jaollinen m:llä ja $(c,\, m) = 1$, on $a - b$ jaollinen m:llä eli $a \equiv b \bmod m$.

Kohdan 2 lauseen perusteella saadaan yleisemmin: Jos $ac \equiv bc \bmod m$ ja $(c,\, m) = d$, niin $a \equiv b \bmod \dfrac{m}{d}$.

Kongruenssien avulla saadaan helposti muutamia yleisiä *jaollisuustarkistimia*. Koska on voimassa $10 \equiv 1 \bmod 3$ ja $\bmod\ 9$, niin

$$a_k 10^k + a_{k-1} 10^{k-1} + \ldots + a_1 10^1 + a_0 \equiv a_k + a_{k-1} + \cdots + a_1 + a_0 \bmod 3$$

ja $\bmod\ 9$. Tästä seuraa erityisesti, että luku on jaollinen kolmella tai yhdeksällä silloin ja vain silloin, kun sen kymmenjärjestelmäesityksen numeroiden summa on jaollinen 3:lla tai 9:llä.

Koska $10 \equiv -1 \bmod 11$, päätellään samoin, että luku n on jaollinen 11:llä jos ja vain jos luku, joka saadaan kun n:n kymmenjärjestelmäesityksen ensimmäisestä numerosta vähennetään toinen, lisätään kolmas jne. on jaollinen 11:llä.

Emme tässä laajemmin puutu mielenkiintoisiin kysymyksiin siitä, mitä mahdollisuuksia luvulla $x^k \bmod n$ on, kun $k > 1$. Tehtävänratkaisussa käytetään usein hyödyksi sitä, että $x^2 \equiv 0$ tai $\equiv 1 \bmod n$, kun $n = 3$ ja $n = 4$.

11. Kongruenssiyhtälön ratkaisu. Sanomme, että x on kongruenssiyhtälön $ax \equiv b \bmod m$ *varsinainen ratkaisu*, jos $ax \equiv b$ ja $0 \leq x < m$.

Lause. *Jos* $(a,\, m) | b$, *niin yhtälöllä* $ax \equiv b \bmod m$ *on* $(a,\, m)$ *kappaletta varsinaisia ratkaisuja. Jos* $(a,\, m)$ *ei ole* b*:n tekijä, yhtälöllä ei ole ratkaisuja.*

Todistus. Etsitään x ja y siten, että $ax - b = my$ eli $ax - my = b$. Jos (a, m) ei ole tekijänä luvussa b, tällaisia lukuja ei ole (kohta 10). Jos $(a, m)|b$, merkitään $(a, m) = d$. Olkoon x_0, y_0 se yhtälön $\frac{a}{d}x - \frac{m}{d}y = \frac{b}{d}$ ratkaisu, jolle x_0 on ei-negatiivinen ja pienin mahdollinen. Silloin $x_0 < \frac{m}{d}$ ja x_0, $x_0 + \frac{m}{d}$, $x_0 + 2\frac{m}{d}$, $\ldots$, $x_0 + (d-1)\frac{m}{d}$ ovat varsinaisia ratkaisuja.

Lauseesta seuraa erityisesti, että jos $(a, m) = 1$, niin yhtälöllä $ax \equiv 1 \bmod m$ on ratkaisu x. Se on a:n *käänteisluku* mod m.

Fermat'n (pieni) lause on monesti käyttökelpoinen jaollisuustehtävissä. *Olkoon p alkuluku ja a kokonaisluku, jolle pätee $(a, p) = 1$. Silloin*

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

Todistus. Oletetaan ensin, että a on positiivinen ja todistetaan, että p on luvun $a^p - a = a(a^{p-1} - 1)$ tekijä; koska $(a, p) = 1$, p on tällöin myös luvun $a^{p-1} - 1$ tekijä. Jos $a = 1$ niin $a^p - a = 0$ ja varmasti $p|(a^p - a)$. Olkoon $a \geq 1$ ja $p|(a^p - a)$. Tarkastellaan lukuja $k!\binom{p}{k} = p(p-1)\ldots(p-k+1)$. Nyt $p|k!\binom{p}{k}$, mutta jos $k < p$, niin p ei ole tekijänä luvussa $k!$. Siis $p|\binom{p}{k}$, joten p jakaa luvun

$$(a+1)^p - a^p - 1 = \sum_{k=1}^{p-1} \binom{p}{k} a^k = (a+1)^p - (a+1) - (a^p - a).$$

Induktioaskel on näin otettu. Negatiivisia a:n arvoja koskeva tulos seuraa parittomilla p:n arvoilla suoraan tästä; jos taas $p = 2$, on $a^p - a = a(a-1)$; tämä on jaollinen kahdella koska a tai $a - 1$ on parillinen. □

Jos $(a, p) = 1$ ja p on alkuluku, voidaan kongruenssiyhtälö $ax \equiv b \bmod p$ ratkaista Fermat'n lauseen avulla:

$$x \equiv a^{p-1}x \equiv a^{p-2}(ax) = a^{p-2}b \bmod p.$$

12. Eulerin funktio ja lause. Olkoon $\phi(n)$ niiden lukujen a, $1 \leq a < n$ lukumäärä, joille pätee $(a, n) = 1$. Täten esimerkiksi $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$ ja $\phi(5) = 4$. Positiivisten kokonaislukujen joukossa määritelty funktio ϕ on *Eulerin funktio*.

Lause. *Jos luvun n eri alkutekijät ovat p_1, p_2, $\ldots$, p_k, niin*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

Todistus. Käytetään ns. inkluusion ja ekskluusion periaatetta. Lukujen 1, 2, ..., n joukossa on tasan $\frac{n}{p_i}$ sellaista lukua, joka on jaollinen p_i:llä. Poistetaan joukosta tällaiset, kun $i = 1, 2, \ldots, k$. Jäljelle jäisi

$$n - n\left(\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_k}\right)$$

lukua. Nyt on kuitenkin tullut poistetuksi kaikki p_ip_j:llä jaolliset luvut kahteen kertaan. Lisätään nämä; nyt luvuiksi a, $(n, a) = 1$ on ehdolla

$$n - n\left(\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_k} + \frac{1}{p_1p_2} + \frac{1}{p_1p_3} + \cdots + \frac{1}{p_{k-1}p_k}\right)$$

lukua. Muotoa $p_ip_jp_l$ olevat luvut ovat tulleet lisätyiksi kahdesti, joten ne on vähennettävä jne. Lopulta

$$\phi(n) = n - n\sum\frac{1}{p_i} + n\sum\frac{1}{p_ip_j} - \cdots \pm \frac{n}{p_1p_2\cdots p_k}.$$

Kun summa kirjoitetaan tulomuotoon, saadaan väite. □

Lause. *Jos* $(a, n) = 1$*, niin* $a^{\phi(n)} \equiv 1 \bmod n$*.*

Todistus. Olkoot $1 = r_1 < r_2 < \ldots < r_{\phi(n)} = n - 1$ ehdon $(r_i, n) = 1$ toteuttavat luvut. Olkoon $ar_i = q_i \bmod n$, $0 \le q_i < n$. Jos $q_i \equiv q_j$, on $ar_j \equiv ar_i \bmod n$ ja kohdan 10 perusteella $r_i \equiv r_j$ eli $r_i = r_j$. Tämän vuoksi

$$\{q_1, q_2, \ldots, q_{\phi(n)}\} = \{r_1, r_2, \ldots r_{\phi(n)}\}.$$

Siis myös

$$r_1r_2 \cdot \ldots \cdot r_{\phi(n)} \equiv (ar_1)(ar_2)\ldots(ar_{\phi(n)}) \equiv a^{\phi(n)}r_1r_2\ldots r_{\phi(n)} \bmod n.$$

Koska $(r_1r_2\ldots r_{\phi(n)}, n) = 1$, saadaan edellä esitetyn kongruenssien jakolaskuominaisuuden perusteella $1 \equiv a^{\phi(n)} \bmod n$. □

Jos p on alkuluku, on $\phi(p) = p - 1$, ja Eulerin lause antaa Fermat'n lauseen (joka siis on tullut tässä uudelleen ja eri tavalla todistetuksi).

Eulerin lausetta voidaan käyttää lineaaristen kongruenssien ratkaisemiseen samoin kuin Fermat'n pientä lausetta: jos $(a, n) = 1$, niin kongruenssilla $ax \equiv b \bmod n$ on ratkaisu $x = ba^{\phi(n)-1}$.

13. Kiinalainen jäännöslause. *Jos* $a_1, a_2, \ldots, a_n$ *ovat kokonaislukuja, jotka ovat pareittain yhteistekijättömiä* ($(a_i, a_j) = 1$*, kun* $i \ne j$*), jos* $a = \prod_{i=1}^{n} a_i$ *ja jos* $b_1, b_2, \ldots, b_n$ *ovat mielivaltaisia kokonaislukuja, niin on olemassa (ja modulo* a *vain yksi) luku* x*, jolle on pätevät yhtälöt*

$$x \equiv b_i \bmod a_i, \quad i = 1, 2, \ldots, n.$$

Todistus. Merkitään $c_i = \dfrac{a}{a_i}$. Silloin $(c_i, a_i) = 1$. Olkoon vielä d_i c_i:n käänteisluku mod a_i, siis yhtälön $c_i x \equiv 1 \bmod a_i$ ratkaisu. Tarkastellaan lukua $x = c_1 d_1 b_1 + c_2 d_2 b_2 + \cdots + c_n d_n b_n$. Olkoon j mielivaltainen indeksi 1:n ja n:n väliltä. Nyt, jos $i \neq j$, niin a_j on c_i:n tekijä. Edellisen summan muut termit kuin $c_j d_j b_j$ ovat jaollisia a_j:llä. Lisäksi $c_j d_j \equiv 1 \bmod a_j$. Siis $x \equiv b_j \bmod a_j$. Luku x toteuttaa siis jokaisen kongruenssiyhtälön. Jos kaksi eri lukua toteuttavat kaikki kongruenssiyhtälöt, niiden erotus on jaollinen a:lla. □

14. Pythagoraan luvut. Kokonaislukukolmikon (x, y, z) jäsenet ovat *Pythagoraan lukuja*, jos

$$x^2 + y^2 = z^2.$$

Tunnetuimpia esimerkkejä Pythagoraan luvuista ovat lukukolmikot $(3a, 4a, 5a)$ ja $(5a, 12a, 13a)$.

Pythagoraan lukuja voidaan tuottaa äärettömän monta kaavojen

$$x = (m^2 - n^2)p, \quad y = 2mnp, \quad z = (m^2 + n^2)p, \tag{1}$$

missä m, n ja p ovat kokonaislukuja, avulla. Kaikki Pythagoraan luvut ovat toisaalta muotoa (1).

Lause. *Jos $a^2+b^2 = c^2$ ja a, b ja c ovat yhteistekijättömiä, niin on olemassa kokonaisluvut m ja n , $(m, n) = 1$, siten, että $\{a, b\} = \{m^2 - n^2, 2mn\}$ ja $c = m^2 + n^2$.*

Todistus. Oletuksen mukaan kaikki luvut a, b, c eivät ole parillisia. Jos a ja b olisivat molemmat parittomia, olisi c parillinen ja c^2 jaollinen 4:llä. Toisaalta olisi $a^2 \equiv b^2 \equiv 1 \bmod 4$ ja siis $c^2 \equiv 2 \bmod 4$. Luvuista a ja b toinen on siis parillinen ja toinen pariton. Olkoon a pariton ja b parillinen. Nyt $b^2 = (c-a)(c+a)$. Molemmat $t = c-a$ ja $u = c+a$ ovat parillisia. Koska $2c = t+u$ ja $2a = u-t$, luvuilla t ja u ei ole muita yhteisiä tekijöitä kuin 2. Siis $t = 2m'$ ja $u = 2n'$, $(m', n') = 1$. Koska $b^2 = tu = 4m'n'$, lukujen m' ja n' on oltava neliölukuja, $m' = m^2$, $n' = n^2$. □

15. Wilsonin lause. *Luku $(p-1)!+1$ on jaollinen p:llä jos ja vain jos p on alkuluku.*

Todistus. Jos p ei olisi alkuluku, sillä olisi tekijä, joka olisi $\leq p-1$. $(p-1)!$ on jaollinen tällä tekijällä, joten myös 1 olisi tällä tekijällä jaollinen. Oletetaan sitten, että p on alkuluku. Tarkastellan lukuja $1, 2, \ldots, p-1$. Millään näistä luvuista ei ole yhteistä tekijää p:n kanssa, joten jokaisella on käänteisluku mod p. Jos jonkin näistä luvuista, esimerkiksi a:n, käänteisluku on luku itse, niin $a^2 \equiv 1 \bmod p$ eli $(a-1)(a+1) \equiv 0 \bmod p$. Luvuista $a-1$ ja $a+1$ ainakin toisen on oltava p:llä jaollinen. Näin on jos ja vain jos $a = 1$ tai $a = p$. Muille luvuille luku ja käänteisluku ovat eri lukuja. Mutta se merkitsee, että tulon $(p-1)!$ luvut voidaan, lukuun ottamatta lukuja 1 ja $p-1$, ryhmitellä pareiksi a, b siten, että $ab \equiv 1 \bmod p$. Siis $(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \bmod p$. □