Merkintöjä

$\mathbb{N} = \{1,2,3,\dots\}$ (luonnolliset luvut)
$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ (kokonaisluvut)

1. JAOLLISUUS, ALKUTEKIJÖIHIN JAKO JA S.Y.T.

Määr. Olk. $a, b \in \mathbb{Z}$. Luku a *jakaa* luvun b (eli a on b:n *tekijä*) jos
$b = ka$, missä $k \in \mathbb{Z}$.
Tällöin merkitään $a \mid b$.

Esim. $3 \mid 6$, $0 \mid 0$, $2 \nmid 5$ ('ei jaa'), $81 \mid 124$, $7 \nmid 47$.

Huom. jatkossa $a, b, \dots, x, y, \dots$ ovat aina kokonaislukuja ellei toisin mainita!

Lause 1.1 (i) jos $c \mid b$ ja $b \mid a$, niin $c \mid a$.

(ii) jos $a \mid b \Rightarrow a \mid bc$ kaikilla c

(iii) jos $a \mid b_1, \dots, a \mid b_n \Rightarrow a \mid (b_1 + \dots + b_n)$

Tod. HT

Määr. Jos $p \in \mathbb{N}$, $p \geq 2$ ja ehdosta $k \mid p$, $k \in \mathbb{N}$ seuraa $k \in \{1, p\}$, sanomme että p on alkuluku. Merkitään $p \in P$. Siis

$$P = \{2, 3, 5, 7, \dots\}$$

Määr. Luvut $m \geq 2$, $m \notin P$, ovat yhdistettyjä lukuja.

[Lause 1.2. Jokainen luonnollinen luku (≥ 2) on esitettävissä alkulukujen tulona.

Tod. Vastaoletus: olkoon n pienin kokonaisluku, $n > 1$, jota ei voi esittää alkulukujen tulona. Erityisesti $n \notin P$, joten $n = n_1 n_2$, missä $n_1, n_2 > 1$. Nyt n_1 ja n_2 ovat alkulukujen tuloja, joten n on myös. ↯ ← ristiriidan merkki! □

[Lause 1.3 (Euklides, n. 300 e.a.a) On olemassa ääretön monta alkulukua.

Tod. Vastaoletus: $P = \{p_1, p_2, \ldots, p_k\}$.
Merk. $m = p_1 p_2 \cdots p_k + 1$.
Silloin $p_j \nmid m$, $1 \leq j \leq k$. Lauseen 1.2 nojalla on olemassa $p \in P$ jolle $p \mid m$, mikä on mahdotonta. ↯ □

[Lause 1.4. (jakojäännöslause) Olkoon $b \geq 1$ ja $a \in \mathbb{Z}$. Silloin on olemassa yksikäs. luvut $q, r \in \mathbb{Z}$ joille $a = qb + r$, $0 \leq r < b$.

Tod. Merkitään

$$U = \{a - ub \mid a - ub \geq 0,\ u \in \mathbb{Z}\}$$

Selvästi U on epätyhjä (miksi?) Olkoon r joukon U pienin alkio, ja kirjoitetaan $r = a - u_1 b$. Siis $r \geq 0$. Jos $r \geq b$, niin

$$a - (u_1 + 1)b = r - b \geq 0,$$

mikä on vastoin r:n määritelmää. Siis $0 \leq r < b$ ja voimme valita $q = u_1$.

Yksikäsitteisyys: jos $0 \le r_1, r_2 < b$, ja
$r_1 = a - u_1 b$, $r_2 = a - u_2 b$, niin

$b \mid (r_1 - r_2)$. Jos $r_1 \neq r_2$, tästä seuraa $|r_1 - r_2| \ge b$, mikä ei ole mahdollista koska $-b < r_1 - r_2 < b$. □

Seuraava tulos voi tuntua ilmeiseltä, mutta kun asiaa mietti tarkasti (tee se!), se osoittautuukin varsin syvälliseksi havainnoksi.

Lause 1.5. Olkoon $a \neq 0$ tai $b \neq 0$. On olemassa 1-käsitteinen kokonaisluku d (lukujen a ja b 'suurin yhteinen tekijä'), jolle pätee:
(i) $d \mid a$ ja $d \mid b$
(ii) jos $d' \mid a$ ja $d' \mid b$ $\Rightarrow$ $d' \mid d$
(iii) $d \ge 1$

Tod. Määritellään suoraan

(1) $$d = \min\{ax + by \mid ax + by \ge 1,\ x, y \in \mathbb{Z}\},$$

eli d on lukujoukon $\{ax + by \mid x, y \in \mathbb{Z}\}$ (selvästi epätyhjän) pienin positiivinen alkio.
Olkoon $d = ax_0 + by_0$ jollakin $x_0, y_0 \in \mathbb{Z}$.
Selvästi d toteuttaa ehdot (iii) ja (i) (mikä jälkimmäinen?). Ehdon (i) todistamiseksi oletetaan, että $d \nmid a$. Silloin jakojäännöslauseen nojalla $a = dq + r$, $0 < r < d$. Saadaan

$$1 \le r = a - dq = a(1 - qx_0) + b(-qy_0) < d,$$

mikä on vastoin d:n määritelmää. Siis $d \mid a$ ja vastaavasti näytetään, että $d \mid b$.

Yksikäsitteisyys seuraa ehdoista (i) ja (ii):
jos d_1 ja d_2 toteuttavat (i)–(iii), niin
$d_1, d_2 \ge 1$, $d_1 \mid d_2$ ja $d_2 \mid d_1 \Rightarrow d_1 = d_2$. □

Määr. • a:n ja b:n suurinta yhteistä tekijää merkitään s.y.t(a,b), tai yksinkertaisemmin (a,b).

• jos $(a,b)=1$ ovat a ja b *suhteellisia alkulukuja* (eli keskenään jaottomia).

Seuraus 1.6. Olkoon $a \neq 0$ tai $b \neq 0$ ja $d=(a,b)$. Silloin

(i) $d = x_0 a + y_0 b$ joillakin $x_0, y_0 \in \mathbb{Z}$.

(ii) $\{xa+yb \mid x,y \in \mathbb{Z}\} = \{kd \mid k \in \mathbb{Z}\}$

Tod. (i) seuraa suoraan määritelmästä (1) s. 5.

(ii) Edellisen kohdan nojalla "vasen puoli" $\supset$ "oikea puoli". Toinen suunta seuraa lauseen 1.5 kohdasta (i). □

Esim. $(8,22)=2$, $2 = -8\times 8 + 3\times 22$.

Seuraus 1.7. Jos $a \mid bc$ ja $(a,b)=1$, niin $a \mid c$

Tod. Seur. 1.6 $\Rightarrow \exists x_0, y_0$ joille $1 = x_0 a + y_0 b$. Nyt $c = acx_0 + bcy_0$, ja tässä $a \mid acx_0$ ja $a \mid bcy_0$. □

Seuraus 1.8. Jos $p \in P$ ja $p \mid ab$, niin $p \mid a$ tai $p \mid b$.

Tod. Ilmeinen. □

Induktiolla seuraa edellisestä (HT):

jos $p \mid q_1 \cdots q_k \Rightarrow p \mid q_j$ jollakin j.

[**Seuraus 1.9.** Jos $p \mid q_1 \cdots q_k$, $p, q_1, \ldots, q_k \in P$, niin $p = q_j$ jollakin $1 \le j \le k$.

Tod. Nyt $p \mid q_j \Leftrightarrow p = q_j$ koska $p, q_j \in P$. □

Olemme nyt valmiit todistamaan aritmetiikan peruslauseen:

[**Lause 1.10.** (Alkutekijöihin jaon 1-käsitteisyys) Jokainen positiivinen kokonaisluku $n \ge 2$ voidaan kirjoittaa muodossa

$$n = p_1 p_2 \cdots p_r \quad , \quad r \ge 1 \, ,$$

missä $p_1, \ldots, p_r \in P$ ja esitys on 1-käsitteinen tekijöiden järjestystä lukuunottamatta.

Tod. Lauseen 1.2 nojalla jokainen $n \ge 2$ voidaan esittää alkulukujen tulona. Olkoon $n \ge 2$ pienin luku jolla on <u>eri</u> esitykset

$$n = \prod_{j=1}^{m} p_j^{\alpha_j} = \prod_{j=1}^{m} p_j^{\beta_j} \quad , \quad \alpha_j, \beta_j \ge 0$$

(Tässä $p_1, \ldots, p_m$ ovat eri alkulukuja – ne jotka esiintyvät jommassa kummassa esityksessä. Huomaa, että α_j:t ja β_j:t voivat saada arvon nolla). Olkoon esim. $\alpha_1 \ge \beta_1$. Tällöin $\beta_1 = 0$, koska muuten $n / p_1^{\beta_1}$ olisi pienempi luku jolla on kaksi eri esitystä. Tällöin

$$p_1 \mid \prod_{j=2}^{m} p_j^{\beta_j} \, ,$$

mikä on mahdotonta seuraus 9:n nojalla koska $p_j \ne p_1$ kun $j \ge 2$.

Määr. Olkoot $a_1, \dots, a_n$ kokonaislukuja (eivät kaikki nollia). Silloin

$$d = s.y.t.(a_1, \dots, a_n) = (a_1, \dots, a_n)$$

on se 1-käsitteinen kokonaisluku, jolle

(i) $d \mid a_k$ kun $k = 1, \dots, n$

(ii) jos $d' \mid a_k$ kun $k = 1, \dots, n$, niin $d' \mid d$

(iii) $d > 0$.

$s.y.t.(a_1, \dots, a_n)$:n olemassaolo on HT.

Aritmetiikan peruslauseen nojalla jokainen $n \in \mathbb{N}$ voidaan kirjoittaa yksikäsitteisesti muotoon

$$n = \prod_{k=1}^{\infty} p_k^{\alpha_k}, \quad \alpha_k \geq 0,$$

missä $p_1 = 2, p_2 = 3, p_3 = 5, \dots$ ovat alkuluvut kasvavassa järjestyksessä ja $\alpha_k = \alpha_k(n) = 0$ suurilla k. Jos $m = \prod_{k=1}^{\infty} p_k^{\beta_k}$, niin (HT)

$$(n, m) = \prod_{k=1}^{\infty} p_k^{\gamma_k}, \text{ missä } \gamma_k = \min(\alpha_k, \beta_k).$$

Lause 1.11 Olk. $a, b \geq 1$. On olemassa luku

$$h = p.y.j.(a, b) \quad (\text{'pienin yhteinen jaettava'})$$

jolle

(i) $a \mid h$, $b \mid h$

(ii) $a \mid h'$, $b \mid h' \Rightarrow h \mid h'$

(iii) $h \geq 1$

Tod. HT.

Huom. Pätee kaava $p.y.j.(a, b) = \dfrac{ab}{(a, b)}$ (HT).

Sovellus: 2. muuttujan lineaarinen Diofantoksen yhtälö

Lause 1.12. Olkoon $a \neq 0$ tai $b \neq 0$. Yhtälöllä

$$ax + by = c$$

on kokonaisratkaisu jos ja vain jos $d \mid c$, missä $d = (a,b)$. Jos (x_0, y_0) on jokin ratkaisu, kaikki ratkaisut saadaan kaavasta

$$\begin{cases} x = x_0 + \frac{b}{d}t \\ y = y_0 - \frac{a}{d}t \end{cases}, \quad t \in \mathbb{Z}.$$

Tod. Jos ratkaisu on olemassa, selvää suoraan yhtälöstä, että $d \mid c$. Käänteen, jos $d \mid c$, voimme jakaa yhtälön kertoimet d:llä, eli yhtäpitävästi

$$a'x + b'y = c',$$

missä $a' = a/d$, $b' = b/d$ ja $c' = c/d$. Tällöin $(a', b') = 1$ (HT). Riittää siis tarkastella tapausta $d = 1$.

Oletetaan, että $d = 1$. Seurauksen 1.6 nojalla on olemassa x_1, y_1 joille $ax_1 + by_1 = 1$. Silloin $acx_1 + bcy_1 = c$, eli pari x_0, y_0 on ratkaisu kun valitaan $x_0 = cx_1$, $y_0 = cy_1$. Olkoon x, y toinen ratkaisu. Silloin

$$ax + by = ax_0 + by_0,$$

eli $a(x - x_0) = -b(y - y_0)$. Koska $(a,b) = 1$ seuraa tästä (Seur. 1.7) $b \mid (x - x_0)$, eli $x = x_0 + tb$ jollakin $t \in \mathbb{Z}$. Tällöin $y = y_0 - ta$. Käänteen, tällaiset parit toteuttavat aina yhtälön. □

Edellisen lauseen antaa ratkaisun teoriassa. Miten käytännössä ratkaisemme vaikkapa yhtälön

$$127x - 87y = 1.$$

Yksi mahdollisuus on kokeilla x:n paikalle luvut $1, 2, \ldots, 87$ ja katsoa milloin yhtälö tulee tosiseksi (mieti miksi riittää kokeilla näin?). Nopeamman ratkaisun pääsee soveltamalla (myös teoreettisesti tärkeää) Euklideen algoritmia:

EUKLEIDEEN ALGORITMI (a, b):n etsimiseksi: Kirjoitetaan jakojäännöslauseen nojalla peräkkäin (oletamme $a > b \geq 1$)

$$\begin{aligned}
a &= bq_1 + r_1, & 0 < r_1 < b \\
b &= r_1 q_2 + r_2, & 0 < r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3, & 0 < r_3 < r_2 \\
&\vdots & \vdots \\
r_{k-2} &= r_{k-1} q_k + r_k, & 0 < r_k < r_{k-1} \\
r_{k-1} &= q_{k+1} r_k & \text{(jako menee taas ensimmäisen kerran)}
\end{aligned}$$

[Lause 1.13 $r_k = (a, b)$.

Tod Viim. yht. $\Rightarrow$ $r_k \mid r_{k-1}$, jolloin

2. viim. yht $\Rightarrow$ $r_k \mid r_{k-2}$,

3. viim. yht $\Rightarrow$ $r_k \mid r_{k-3}$,

$\vdots$

2. yhtälö $\Rightarrow$ $r_k \mid b$

1. yhtälö $\Rightarrow$ $r_k \mid a$.

Käänteen, jos $d=(a,b)$, niin

1. yht. $\Rightarrow d \mid r_1$, 2. yht. $\Rightarrow d \mid r_2$,
..., 2. viim. yhtälö $\Rightarrow d \mid r_k$.

Siis $r_k \mid a$, $r_k \mid b$ ja $d \mid r_k$, $r_k \geq 1$, eli $r_k = d$. □

Euklideen algoritmia voi myös soveltaa yhtälön $ax+by=d=(a,b)$ ratkaisemiseen:

1. yht. $\Rightarrow r_1 = a - bq_1 \overset{\text{merk.}}{=} u_1 a + v_1 b$

2. yht. $\Rightarrow r_2 = b - q_2(u_1 a + v_1 b) = u_2 a + v_2 b$

$\vdots$ $\qquad\qquad\qquad\qquad\qquad\qquad$ $\vdots$

2. viim yht. $\Rightarrow d = r_k = r_{k-2} - r_{k-1} q_k$

$= (u_{k-2} a + v_{k-2} b) - q_k (u_{k-1} a + v_{k-1} b)$

$= x_0 a + y_0 b$.

Tietenkään käytännössä ei tarvitse harrastaa yo. kompleksia notaatiota.

Esim. $(127,87)=1$. Tarkistetaan tämä Euklideen algoritmin avulla:

$$127 = 87 \cdot 1 + 40 \quad , \quad 87 = 40 \cdot 2 + 7$$
$$40 = 7 \cdot 5 + 5 \quad , \quad 7 = 5 \cdot 1 + 2$$
$$5 = 2 \cdot 2 + 1 \quad ; \quad (127,87) = 1.$$

Ratkaistaan sitten yhtälö $127x - 87y = 1$ (vrt. s. 10.). Merkitään $127=a$ ja $87=b$ ja ratkaistaan peräkkäin:

$$40 = a-b, \quad 7 = b - 2(a-b) = 3b-2a,$$

$$5 = (a-b) - 5(3b-2a) = 11a-16b$$

$$2 = (3b-2a) - (11a-16b) = 18b-13a$$

$$1 = (11a-16b) - 2(18b-13a) = \underline{37a-54b}$$

Löysimme ratkaisun $(x_0, y_0) = (+37, +54)$, jolloin yhtälön $127x - 87y = 1$ yleinen ratkaisu on

$$\begin{cases} x = 37 + k\,87 \\ y = 54 + k\,127 \end{cases}, \quad k \in \mathbb{Z}.$$

Eukleideen algoritmi voi vaikuttaa kömpelöltä, mutta itseasiassa se on varsin tehokas suurilla luvuilla:

Lause 1.14 Eukleideen algoritmin tarvitsema askelmäärä $\leq 3 \log a + 2$ (kun $a \geq b$)

Tod. HT □

(2) KONGRUENSSIT JA RENGAS $\mathbb{Z}_m$.

Gauss otti käyttöön kongruenssin käsitteen. Se helpottaa huomattavasti jaollisuustarkasteluja.

Määr. Olkoon $m \neq 0$. Jos $m \mid (a-b)$, sanomme että a on kongruentti b:n kanssa modulo m. Merkitsemme tällöin $a \equiv b \pmod{m}$.
('modoli')

Huom. Lyhyesti sanoen siis
$$a \equiv b \pmod{m} \iff m \mid (a-b).$$

Seuraava havainto osoittaa, että $\equiv$ on ekvivalenssirelaatio!

Lause 2.1. Kongruenssi (mod m) toteuttaa:
(i) $a \equiv a \pmod{m}$
(ii) $a \equiv b \iff b \equiv a \pmod{m}$
(iii) $a \equiv b$ ja $b \equiv c \Rightarrow a \equiv c \pmod{m}$.

Tod. Seuraa suoraan määritelmästä.

Seuraavat kolme lausetta sisältävät kongruenssien peruslaskusäännöt:

Lause 2.2. (i) Jos $a \equiv b \pmod{m}$, niin kaikilla k pätee $a+k \equiv b+k$ ja $ka \equiv kb \pmod{m}$
(ii) Jos $a \equiv b$ ja $c \equiv d \pmod{m}$, niin
$a+c \equiv b+d \pmod{m}$ ja $ac \equiv bd \pmod{m}$

Tod. Seuraava helposti määritelmästä (tee!), viimeistä väitettä varten on hyödyllistä havaita $ac - bd = a(c-d) + d(a-b)$. □

Lause 2.3. Jos $P(x)$ on kokonaiskertoiminen polynomi, niin $a \equiv b \pmod m \Rightarrow P(a) \equiv P(b) \pmod m$.

Tod. Olkoon $P(x) = a_0 + a_1 x + \dots + a_n x^n$.
Iteroimalla edellistä lausetta saamme
$a^k \equiv b^k \pmod m$ kaikilla $k \geq 0$.

Erityisesti $a_j a^k \equiv a_j b^k \pmod m$, $k = 0, 1, \dots, n$.
Väite seuraa summaamalla yli $k:n$, $k = 0, 1, \dots, n$. □

Vastaavanti todistetaan:

Lause 2.4. Jos P on $k:n$ muuttujan kokonaiskertoiminen polynomi, niin

$$P(x_1, \dots, x_k) \equiv P(y_1, \dots, y_k) \pmod m$$

mikäli $x_j \equiv y_j \pmod m$ kun $j = 1, \dots, k$.

Esim. $7 \equiv -13 \pmod{20}$
$200 \equiv -10 \pmod 3$

Esim Osoita, että luku
$n = 52(169^9 + 87^7) + 6$ on jaollinen luvulla 11.

Ratk. $169 \equiv 4 \pmod{11}$, $52 \equiv 8 \pmod{11}$,
$87 \equiv -1 \pmod{11}$.

Lisäksi

$4^2 = 16 \equiv 5$, $4^4 = 5^2 \equiv 3$, $4^8 \equiv 3^2 = 9 \pmod{11}$,
sitten $4^9 \equiv 36 \equiv 3 \pmod{11}$. — Saamme

$$n \equiv 8 - (3 + (-1)^7) + 6 = 8 - 2 + 6 = 22 \equiv 0 \pmod{11}. \quad \square$$

Huom. Laskettaessa $a^k \equiv ? \pmod{m}$, on edullista laskea ensin peräkkäisten suureet a^1, a^2, a^4, a^8 jne ja lausua annettu potenssi näiden tulona. Esim.

$$a^{23} = a^{16} \cdot a^4 \cdot a^2 \cdot a^1.$$

Esim. Patee $10 \equiv 1 \pmod{9}$, jotenkin jos

$S(n) :=$ luvun n numeroiden summa, niin

saamme $9 \mid n \iff 9 \mid S(n) \iff 9 \mid S(S(n))$ jne..

Esim. Olkoon $n = 5476289$. Silloin
$S(n) = 5+4+7+6+2+8+9 = 41$, $S(S(n)) = 5 \not\equiv 0 \pmod{9}$,
jotenkin $9 \nmid n$.

Määr. Jos $a \equiv b$ ei ole voimassa, merkitsemme
$a \not\equiv b \pmod{m}$.

Lyhyt kertaus: Ryhmät, renkaat, kunnat

'kaltaialkio'

Määr. $(S, \circ)$ on ryhmä jos laskutoimitus $\circ$ toteuttaa ($\circ : S \times S \to S$, merkitään $\circ(a,b) = a \circ b$):

(1) $a \circ (b \circ c) = (a \circ b) \circ c \quad \forall a, b, c \in S$. (assosiatiivisuus)

(2) $\exists e \in S$ jolle $a \circ e = e \circ a = a \quad \forall a \in S$.

(3) Jokaiselle $a \in S$ on 'käänteisalkio' $\bar{a} \in S$, jolle $\bar{a} \circ a = a \circ \bar{a} = e$.

Huom. Jos (1) ja (2) voimassa, kyseessä monoidi

Esim (i) $\mathbb{Z}$ (tai $\mathbb{Q}$ tai $\mathbb{R}$) ovat ryhmiä luonnol. lisäyslaskun suhteen.

(ii) $\mathbb{Q} \setminus \{0\}$ on ryhmä kun laskutoimituksena on tavallinen kertolasku.

(iii) $(\{0,1\}, \oplus)$ on kahden alkion ryhmä kun määritellään

$\oplus$	0	1
0	0	1
1	1	0

Määr. $(S,\circ)$ on vaihdannainen (= kommutatiivinen, Abel) ryhmä jos
$$a \circ b = b \circ a \quad \forall\ a,b \in S.$$
← kaksiargumenttinen laskutoimitus

Määr. $(S, +, \cdot)$ on kommutatiivinen rengas, jos

(1) $(S,+)$ on kommutatiivinen ryhmä (merkitään sen neutraalialkiota 0:lla)

(2) $(S,\cdot)$ on kommutatiivinen monoidi (merkitään neutraalialkiota 1:llä)

(3) $1 \neq 0$

(4) $a(b+c) = ab + ac \quad \forall\ a,b,c \in S$ (liitännäisyys)

Määr. $(S,+,\cdot)$ on kunta jos se on kommutatiivinen rengas ja $(S \setminus \{0\}, \cdot)$ on ryhmä (eli jokaisella alkiolla $a \neq 0$ on käänteisalkio laskutoimituksen $\cdot$ suhteen)

Määr. Kommutatiivinen rengas on kokonaisalue jos $ab=0 \Rightarrow a=0$ tai $b=0$.

(Huom. jokainen kunta on kokonaisalue (miksi?))

Esim. $\mathbb{Z}$ on rengas, $\mathbb{Q}$ ja $\mathbb{R}$ (luonnollisilla laskutoimituksilla) ovat kuntia.

Esim. $(\{a,b\}, \oplus, \odot)$ on kunta jos (HT)

$\oplus$	a	b
a	a	b
b	b	a

$\odot$	a	b
a	a	a
b	a	b

($\oplus$:n neutraalialkio on a
$\odot$:n — " — on b)

Meille riittää hyvä intuitiivinen ym. käsitteiden ymmärrys. Myöhemmin tarkastamme lukuteoriaan kuuluvia esimerkkejä.

Jäännösluokkien rengas $\mathbb{Z}_m$

Lauseen 14 mukaan $\equiv$ on ekvivalenssirelaatio. Vastaavia ekvivalenssiluokkia kutsutaan jäännösluokiksi (mod m).

[Lemma 2.5. Jäännösluokkia (mod m) on m kappaletta.

Tod. Jakojäännöslause $\Rightarrow$ jokainen $n \in \mathbb{Z}$ voidaan kirjoittaa muotoon $n = km + r$, $r \in \{0,1,\dots,m-1\}$. Luvut $0,1,\dots,m-1$ ovat selvästi epäkongruentteja. Toisaalta jos $n = km+r$, niin $n \equiv r \pmod m$. □

[Määr. Luvun $a \in \mathbb{Z}$ määräämä jäännösluokka (mod m) on

$$[a] = \{a + km \mid k \in \mathbb{Z}\}.$$

Määr. $\mathbb{Z}_m = \{[a] \mid a \in \mathbb{Z}\} = \{[0],[1],\ldots,[m-1]\}$. *)

Lause 2.6. $(\mathbb{Z}_m, +, \cdot)$ on kommutatiivinen m:n alkion rengas kun yhteenlasku ja tulo määritellään kaavalla

$$[a]+[b] = [a+b], \quad [a][b] = [ab].$$

Tod. Selvästi $\mathbb{Z}_m$:ssä 0-alkio on $[0]$, 1-alkio $[1]$ (esim. $[0]+[a] \overset{\text{määr.}}{=} [0+a] = [a]$). Renkaan määritelmän muut ehdot todetaan vastaavasti. Esim.

$$([a]+[b])[c] \overset{\text{määr.}}{=} [a+b][c] \overset{\text{määr.}}{=} [(a+b)c] = [ac+bc]$$
$$\overset{\text{määr.}}{=} [ac]+[bc] \overset{\text{määr.}}{=} [a][c]+[b][c].$$

Muut vastaavasti. Mutta, olemaisia on tarkistaa, että tulon ja summan määritelmät ovat hyvin asetettuja, eli että ne eivät riipu käytetyistä jäännösluokkien edustajista. Olkoon siis

$$[a] = [a'] \quad \text{ja} \quad [b] = [b'],$$

eli $a \equiv a'$ ja $b \equiv b' \pmod m$. Lauseen 2.2 nojalla silloin

$$a+b \equiv a'+b' \quad \text{ja} \quad ab \equiv a'b' \pmod m,$$

joten $[a+b] = [a'+b']$ ja $[ab] = [a'b']$. □

Määr. Jakojäännöslause $\Rightarrow$ $n \in \mathbb{Z}$ void. kirj. $n = qm+r$, $0 \le r \le m-1$. Sanomme, että r on luvun n **pienin positiivinen jäännös** $\pmod m$.

Esim. • $\mathbb{Z}_5$:ssä $[3][6] = [18] = [3]$, $[-5] = [0]$.

• Luvun -23 pienin positiivinen jäännös $\pmod{17}$ on 11 $(-23 = -2\cdot 17 + 11)$

---

*) Oikeampi merkintä jäännösluokkien renkaalle olisi $\mathbb{Z}/m\mathbb{Z}$!

- $\mathbb{Z}_6$: nyt $[2] \neq [0]$, $[3] \neq [0]$, mutta
$$[2][3] = [6] = [0].$$

Siis $\mathbb{Z}_6$ ei ole kokonaisalue, erityisesti se ei ole kunta. Milloin $\mathbb{Z}_m$ on kunta?

Lause 2.7. Olk. $m \geq 2$. $\mathbb{Z}_m$ on kunta jos ja vain jos m on alkuluku.

Tod Jos $m = m_1 m_2$, $2 \leq m_1, m_2 \leq m-1$ (eli $m \notin P$), niin $[m_1] \neq [0] \neq [m_2]$, mutta $[m_1][m_2] = [m] = [0]$, eli tällöin $\mathbb{Z}_m$ ei ole edes kokonaisalue.

Olkoon sitten $m \in P$. Jos $[a] \neq [0]$, niin $[a, m] = 1$. Seurauksen 1.6 nojalla on olemassa x, y joille $xa + ym = 1$, jolloin $xa \equiv 1 \pmod{m}$, eli $[x][a] = [1]$. Siis $[x]$ on $[a]$:n käänteisalkio tulon suhteen. Jokaisella $[0]$:sta eroavalla alkiolla on käänteisalkio tulon suhteen, joten $\mathbb{Z}_m$ on kunta. □

Määr. Olk. $m \geq 1$. Joukko $\{a_1, \ldots, a_m\}$ on täydellinen jäännösjoukko (mod m), mikäli
$$\{[a_1], [a_2], \ldots, [a_m]\} = \mathbb{Z}_m.$$

Lause 2.8. Olkoon $m \geq 2$ ja $U \subset \mathbb{Z}$. Silloin U on täydellinen jäännösjoukko (mod m) jos ja vain jos ainakin kaksi seuraavista ehdoista on voimassa:

(i) U:ssa on m lukua

(ii) U:n alkiot ovat keskenään epäkongruentteja (mod m)

(iii) Jokaisella $a \in \mathbb{Z}$ on olemassa $u \in U$ jolle $a \equiv u \pmod{m}$

Tod. HT. □

Seuraus 2.9. Olkoon $\{a_1, \dots, a_m\}$ täyd. jäännösysteemi $(\bmod m)$, ja $(k,m)=1$, $b \in \mathbb{Z}$. Silloin myös $\{ka_1+b, \dots, ka_m+b\}$ on täyd. jäännösysteemi.

Tod. Riittää näyttää, että Lauseen 2.8 ehdot (i) ja (ii) ovat voimassa. Ehto (i) on ilmeinen. Oletetaan, että $ka_j+b \equiv ka_\ell+b \pmod m$. Silloin $m \mid k(a_j-a_\ell)$, josta (Seur. 1.7) $m \mid (a_j-a_\ell)$, eli $a_j \equiv a_\ell \pmod m$. Täyd. jäännösyst. määr. nojalla $a_j = a_\ell$. □

Seuraava lause on lukuteorian perustuloksia.

Lause 2.10 (Fermat'n pieni lause)

Jos p on alkuluku ja $p \nmid a$, niin $a^{p-1} \equiv 1 \pmod p$.

Tod. $\{0,1,\dots,p-1\}$ on täyd. jäännösysteemi $(\bmod p)$. Koska $(a,p)=1$, samoin on $\{0, a, 2a, \dots, (p-1)a\}$ edellisen Seurauksen nojalla. Siispä luvut $\{a, 2a, \dots, (p-1)a\}$ ovat jossain järjestyksessä kongruentit lukujen $\{1, \dots, p-1\}$ kanssa. Erityisesti

$$1 \cdot 2 \cdot \dots \cdot (p-1) \equiv a \cdot 2a \cdot \dots \cdot (p-1)a \pmod p$$

$$\Leftrightarrow \quad (p-1)! \equiv a^{p-1}(p-1)! \pmod p$$

Koska $((p-1)!, p)=1$, seuraa tästä $1 \equiv a^{p-1} \pmod p$. □

Huom. Sovelsimme edellä helppoa havaintoa:

Lemma 2.11 Jos $ka \equiv kb \pmod m$ ja $(k,m)=1$, niin $a \equiv b \pmod m$.

Tod. HT. □

Seuraus 2.12. Jos $p \geq 2$ on alkuluku, niin
$a^p \equiv a \pmod{p}$ kaikilla $a \in \mathbb{Z}$.

Esim. $p \mid (2^p - 2)$ kaikilla $p \in \mathbb{P}$.

Tehtävä. Olkoon p alkuluku, $p \neq 2, 5$. Osoita, että p jakaa ääretön monta luonnollisten lukujen jonon
$1, 11, 111, 1111, \ldots$ jäsentä.

Ratk. $\underbrace{111\ldots1}_{k \text{ kpl}} = 10^{k-1} + 10^{k-2} + \ldots + 1 = (10^k - 1)/9$.

Tapaus 1. $p \neq 3$. Nyt $p \geq 7$. Riittää osoittaa, että $10^k \equiv 1 \pmod{p}$ äärettömän monella k. Fermat'n pieni lause $\Rightarrow 10^{p-1} \equiv 1 \pmod{p}$, koska $(10, p) = 1$. Korottamalla potenssiin saamme
$10^{\ell(p-1)} \equiv 1 \pmod{p}$ kaikilla $\ell \geq 1$.

Tapaus 2. $p = 3$. Nyt $10^j \equiv 1^j \equiv 1 \pmod{3}$, eli
$10^{k-1} + \ldots + 1 \equiv k \cdot 1 = k \pmod{3}$.

Siispä kyseinen luku on jaollinen kolmella aina kun $3 \mid k$. □

Eulerin φ-funktio ja sovitettuja jäännösryhmäesimerkkejä

Määr. (Eulerin φ-funktio) Asetetaan $\varphi(1) = 1$ ja kun $m \geq 2$, merkitsemme $\varphi(m)$ on niiden luonnollisten lukujen $a \in \{1, 2, \ldots, m\}$ lukumäärä, joille $(a, m) = 1$.

Esim $\varphi(2) = 1$, $\varphi(6) = 2$, $\varphi(7) = 6$, yleisesti $\varphi(p) = p - 1$ jos $p \in \mathbb{P}$.

[Määr. Lukuteor. funktio on kuvaus $F: \mathbb{Z} \to \mathbb{R}$ ($\mathbb{C}$) tai $F: \mathbb{N} \to \mathbb{R}$ ($\mathbb{C}$)

[Määr. Lukuteor. funktio $F: \mathbb{N} \to \mathbb{C}$ on <u>multiplikatiivinen</u> jos $F(mn) = F(m)F(n)$ aina kun $(m,n) = 1$

[<u>Lause 2.13</u> φ on multiplikatiivinen

<u>Tod.</u> Oletetaan, että $m,n \geq 2$ ja $(m,n) = 1$. Tarkastellaan taulukkoa

0	1	2	...	$m-1$
m	$m+1$	$m+2$	...	$2m-1$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$(n-1)m$	$(n-1)m+1$	$(n-1)m+2$	...	$nm-1$

- Johainen pystyrivi koostuu luvuista jotka ovat kongruentteja (mod m). Katsomalla ensimmäistä vaakariviä näemme: on olemassa tasan $\varphi(m)$ pystyriviä joiden kaikki alkiot ovat suhteellisia alkulukuja m:n suhteen. Muiden pystyrivien yhdelläkään luvulla ei ole tätä ominaisuutta.

- Johainen pystyrivi muodostaa täydellisen jäännösryhmän mod n Seurauksen 2.9 ja tiedon $(m,n) = 1$ nojalla. Siis jokaisella pystyrivillä on tarkalleen $\varphi(n)$ suhteellista alkulukua n:n suhteen.

- Yhdistetään ed. havainnot $\Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$ □

Lause 2.14. $\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$ ← tulo yli n:n alkulukujoiden

Tod. Jos $n = p_1^{\partial_1} \cdots p_\ell^{\partial_\ell}$ on n:n alkulukuhajotelma, saamme iteroimalla lausetta 2.13:

$$\varphi(n) = \prod_{j=1}^{\ell} \varphi(p_j^{\partial_j})$$

Luonnista $1, 2, \ldots, p^\partial$ ($\partial \in P$) p:llä jaollisia ovat luvut $p, 2p, \ldots, p^\partial$ joita on $p^{\partial-1}$ kpl. Siis $\varphi(p^\partial) = p^\partial - p^{\partial-1} = p^\partial\left(1 - \frac{1}{p}\right)$. Siis

$$\varphi(n) = \prod_{j=1}^{\ell} p_j^{\partial_j}\left(1 - \frac{1}{p_j}\right) = n \prod_{j=1}^{\ell}\left(1 - \frac{1}{p_j}\right). \quad \square$$

Esim. $\varphi(60) = 60 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 16$

$\varphi(pq) = (p-1)(q-1)$ jos $p, q \in P$ ja $p \neq q$.

INTERMEZZO: Todistus lauseelle 2.13. Oletamme tunnetuksi 'inklusion ja eksklusion periaatteen':

$$\#(A_1 \cup A_2 \cup \ldots \cup A_\ell) = \sum_j \#(A_j) - \sum_{j<k} \#(A_j \cap A_k)$$
$$+ \sum_{j<k<m} \#(A_j \cap A_k \cap A_m) - \ldots + (-1)^{\ell-1} \#(A_1 \cap \ldots A_\ell)$$

Jos $n = p_1^{\partial_1} \cdots p_\ell^{\partial_\ell}$ ($\partial_1, \ldots, \partial_\ell \geq 1$) on n:n alkulukuhajotelma. Ayt. sovelletaan edellistä asettamalla

$$A_j = \{k \in \{1, \ldots, n\} : p_j \mid k\}$$

Silloin $\varphi(n) = n - \#(A_1 \cup \ldots \cup A_\ell)$

Sovitusti $\varphi(A_{j_1} \cap A_{j_2} \cap \ldots A_{j_k}) = \frac{n}{p_{j_1} \cdots p_{j_k}}$

Saamme: $\varphi(n) = n - \sum_{j=1}^{\ell} \frac{n}{p_j} + \sum_{1 \leq j < k \leq \ell} \frac{n}{p_j p_k} - \ldots$

$$+ (-1)^\ell \frac{n}{p_1 \cdots p_\ell} = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_\ell}\right). \quad \square$$