Edelleen $a \equiv_n a'$, $b \equiv_n b'$ $\Rightarrow$ $a-a' \in n\mathbb{Z}$, $b-b' \in n\mathbb{Z}$

$\Rightarrow$ $(a+b)-(a'+b') = (a-a')+(b-b') \in n\mathbb{Z}$,

$$ab - a'b' = ab - a'b + a'b - a'b'$$
$$= \underbrace{(a-a')b}_{\in n\mathbb{Z}} + \underbrace{a'(b-b')}_{\in n\mathbb{Z}} \in n\mathbb{Z}$$

$\Rightarrow$ $a+b \equiv_n a'+b'$, $ab \equiv_n a'b'$. □

Relaatio $\equiv_n$ on nimeltään <u>kongruenssi modulo n</u>; sitä, että $a \equiv_n b$, merk. myös $a \equiv b \pmod n$. Luvun $a \in \mathbb{Z}$ ekv.luokkaa (l. a:n <u>jäännösluokkaa modulo n</u>) merk. $[a]_n = [a] = a_n = \bar{a}$.

$b \in [a]_n \Leftrightarrow b - a \in n\mathbb{Z} \Leftrightarrow \exists q \in \mathbb{Z}$ s.e. $b = a + nq$, joten

$$[a]_n = \{a + nq \mid q \in \mathbb{Z}\} \underset{\text{merk.}}{=} a + n\mathbb{Z} \subset \mathbb{Z}.$$

<u>Määr.</u>: Ekv. luokkien joukko $\mathbb{Z}/\equiv_n = \{[a]_n \mid a \in \mathbb{Z}\}$ on <u>kokonaislukujen modulo n joukko</u>, merk. $\mathbb{Z}_n = \mathbb{Z}/\equiv_n$.

Kun $a \in \mathbb{Z}$, jakoyhtälö $\Rightarrow$ $\exists$ tasan yksi $r \in \{0,1,\dots,n-1\}$ s.e. $a - r \in n\mathbb{Z}$; tällöin $a \equiv r \pmod n$, joten $[a]_n = [r]_n$, ja $[r]_n \neq [r']_n$, kun $r \neq r' \in \{0,1,\dots,n-1\}$.

$\therefore$ $\mathbb{Z}_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$, n alkiota

(siis $\{0,1,\dots,n-1\}$ on (eräs) ekv.luokkien edustajisto).

<u>Esim. 2</u>: $\mathbb{Z}_3 = \{[0], [1], [2]\}$, missä
$[0] = 3\mathbb{Z} = \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\}$
$[1] = 1+3\mathbb{Z} = \{\dots, -8, -5, -2, 1, 4, 7, 10, \dots\}$
$[2] = 2+3\mathbb{Z} = \{\dots, -7, -4, -1, 2, 5, 8, 11, \dots\}$
Myös esim. $\mathbb{Z}_3 = \{\underset{[1]}{[7]}, \underset{[0]}{[33]}, \underset{[2]}{[62]}\}$.

<u>Esim. 3</u>: $a \equiv b \pmod 1 \Leftrightarrow a - b \in \mathbb{Z}$, pätee aina; siis $\mathbb{Z}_1 = \{[0]_1\}$, $[0]_1 = \mathbb{Z}$.

Ed. lemman loppuosan mukaan $[a] = [a']$, $[b] = [b']$ $\Rightarrow$ $[a+b] = [a'+b']$, $[ab] = [a'b']$. $\mathbb{Z}_n$:n alkioille voidaan siis määritellä summa ja tulo $\mathbb{Z}$:n yhteen- ja kertolaskun avulla:

$$[a]+[b]=[a+b] \qquad \forall a,b\in\mathbb{Z}.$$
$$[a]\cdot[b]=[ab]$$

Esim.: $\mathbb{Z}_{12}$:ssa on $[6]+[8]=[6+8]=[14]=[2]$ ja $[6]\cdot[8]=[6\cdot 8]=[48]=[0]$, sillä $14=12+2$ ja $48=4\cdot 12+0$.

Lause: Kaikilla $\alpha,\beta,\gamma\in\mathbb{Z}_n$ on

i) $\alpha+\beta=\beta+\alpha$
ii) $\alpha+(\beta+\gamma)=(\alpha+\beta)+\gamma$
iii) $\alpha+0_n=\alpha$
iv) $\alpha\beta=\beta\alpha$
v) $\alpha(\beta\gamma)=(\alpha\beta)\gamma$
vi) $\alpha\cdot 1_n=\alpha$
vii) $\alpha\cdot(\beta+\gamma)=\alpha\beta+\alpha\gamma$.

Lisäksi viii) jos $\alpha\in\mathbb{Z}_n$, niin $\exists\,\beta\in\mathbb{Z}_n$ s.e. $\alpha+\beta=0_n$.
Kan. surjektiolle $p:\mathbb{Z}\to\mathbb{Z}_n$, $a\mapsto[a]_n$, pätee $p(a+b)=p(a)+p(b)$ ja $p(ab)=p(a)p(b)$ $\forall a,b\in\mathbb{Z}$.

Tod.: i)–vii) seuraavat $\mathbb{Z}$:n vast. ominaisuuksista.
Esim. $\alpha=[a]$, $\beta=[b]$, $\gamma=[c]$ $\Rightarrow$ $\alpha(\beta\gamma)=[a]([b][c])$
$=[a]\cdot[bc]=[a(bc)]=[(ab)c]=[ab][c]=$
$=([a][b])\cdot[c]=(\alpha\beta)\gamma$.
viii):ssa $\beta=[-a]$, jos $\alpha=[a]$. Summan ja tulon määr. $\mathbb{Z}_n$:ssä $\Rightarrow$ p:tä koskevat väitteet. □

Esim. 4: Jaetaan $a=18^2+2^{100}$ 11:llä. Jakojäännös = ?

Ratk.: Lasketaan $\mathbb{Z}_{11}$:ssä: $[a]=[18^2+2^{100}]=$
$=[18^2]+[(2^5)^{20}]=[18]^2+[2^5]^{20}=[18]^2+[32]^{20}$
$=[7]^2+[-1]^{20}=[7^2]+[(-1)^{20}]=[49]+[1]$
$=[5]+[1]=[6]$. Vastaus: 6.

Jäännösluokka $\alpha\in\mathbb{Z}_n$ on käänteinen, jos $\exists\,\beta\in\mathbb{Z}_n$ s.e. $\alpha\beta=1_n$ $(=\beta\alpha)$. Tällöin β on 1-käs. määrätty ($\alpha\beta=1_n=\alpha\beta'\Rightarrow\beta'=(\beta\alpha)\beta'=\beta(\alpha\beta')=\beta$), merk. $\beta=\alpha^{-1}$. Lisäksi merk. $\mathbb{Z}_n^*=\{\alpha\in\mathbb{Z}_n \mid \alpha \text{ käänteinen}\}$.

Lemma: $[a]_n\in\mathbb{Z}_n^*\iff \mathrm{syt}(a,n)=1$.

Tod.: $\exists\,b\in\mathbb{Z}$ s.e. $[a]\cdot[b]=[1]\iff$

$\exists b \in \mathbb{Z}$ s.e. $ab \in 1 + n\mathbb{Z} \iff \exists b, v \in \mathbb{Z}$ s.e. $ab + nv = 1 \iff syt(a,n) = 1$. □

Huom.: Kun $syt(a,n) = 1$, luvut $b, v \in \mathbb{Z}$ s.e. $ab + nv = 1$ löydetään esim. Eukl. algoritmilla. Tällöin $[a]_n^{-1} = [b]_n$.

Esim.: $\mathbb{Z}_{12}^* = \{[1], [5], [7], [11]\}$.

Lause 8': $\alpha \in \mathbb{Z}_n^*$, $\gamma \in \mathbb{Z}_n \Rightarrow$ yhtälöllä $\alpha x = \gamma$ on 1-käs. ratkaisu $x \in \mathbb{Z}_n$, nimittäin $x = \alpha^{-1} \cdot \gamma$.

Tod.: $\alpha \cdot (\alpha^{-1}\gamma) = (\alpha \cdot \alpha^{-1}) \cdot \gamma = 1_n \cdot \gamma = \gamma$;
$\alpha x = \gamma = \alpha x' \Rightarrow x' = (\alpha^{-1}\alpha)x' = \alpha^{-1}(\alpha x') = \alpha^{-1}(\alpha x)$
$= (\alpha^{-1}\alpha)x = x$. □

Seuraus (Lause 6): $a, c \in \mathbb{Z}$, $syt(a,n) = 1 \Rightarrow$ kongruenssilla $ax \equiv c \pmod n$ on 1-käs. ratkaisu $x \in \{0, 1, \dots, n-1\}$. □

Huom.: Ol. $a, n, c, x \in \mathbb{Z}$. Silloin x toteuttaa kongruenssin $ax \equiv c \pmod n \iff \exists y \in \mathbb{Z}$ s.e. (x,y) on lineaarisen Diofantoksen yhtälön $ax + ny = c$ ratkaisu.

Esim. 8: $15x + 11y = 137$. Lasketaan $\mathbb{Z}_{11}$:ssä.
$[15] = [4]$, $3 \cdot 4 = 12 = 11 + 1 \Rightarrow [15]^{-1} = [3] \in \mathbb{Z}_{11}$.
$[15] \cdot [x] = [137] = [5] \iff [x] = [3] \cdot [5] = [15] = [4]$
$\iff x = 4 + 11k$, $k \in \mathbb{Z}$. Vastaava $y = (137 - 15x)/11 =$
$= (77 - 165k)/11 = 7 - 15k$.
$\therefore x, y$ mol. $\geq 0 \iff k = 0 \iff x = 4, y = 7$.

Esim. 7: yhtälöllä $x^2 - 2y^2 = 5$ ei ole ratk. $x, y \in \mathbb{Z}$.

Tod.: Vastaol.: $\exists x, y \in \mathbb{Z}$ s.e. $x^2 - 2y^2 = 5$
$\Rightarrow [x]_8^2 - 2[y]_8^2 = [5]_8$ eli $[x]_8^2 = [5]_8 + 2 \cdot [y]_8^2$.
Laskemalla: $[x]_8^2, [y]_8^2 \in \{[0]_8, [1]_8, [4]_8\}$
(riittää tutkia arvot $x, y = 0, 1, \dots, 7$)
$\Rightarrow 2 \cdot [y]_8^2 \in \{[0]_8, [2]_8\} \Rightarrow [5]_8 + 2[y]_8^2 \in \{[5]_8, [7]_8\}$
$\Rightarrow$ ei voi olla $[5]_8 + 2[y]_8^2 = [x]_8^2 \in \{[0]_8, [1]_8, [4]_8\}$,
RR. □

Samanaikaisten kongruenssien ratkaiseminen

Olkoot $m, n \in \mathbb{N}_+$ (ts. $m, n \geq 1$) ja $k, l \in \mathbb{Z}$.

Tehtävä: Etsittävä kaikki kokonaisluvut $x \in \mathbb{Z}$, jotka toteuttavat molemmat kongruenssit

$$x \equiv k \pmod{m} \quad \text{ja} \quad x \equiv l \pmod{n}.$$

Huom.: Tällaisia lukuja $x \in \mathbb{Z}$ ei välttämättä ole olemassa.

Esim.: $x \equiv 1 \pmod 4$ ja $x \equiv 0 \pmod 6$.
$x \equiv 1 \pmod 4 \Rightarrow x = 1 + 4r$ jollakin $r \in \mathbb{Z}$
$\Rightarrow x$ on pariton;
$x \equiv 0 \pmod 6 \Rightarrow x = 6s$ jollakin $s \in \mathbb{Z}$
$\Rightarrow x$ on parillinen.
Siis sama x ei voi toteuttaa molempia kongruenssejä.

Kiinalainen jäännöslause: Olkoot ykkä m ja n keskenään jaottomat. Silloin kongruenssseilla

$$x \equiv k \pmod m \quad \text{ja} \quad x \equiv l \pmod n$$

on yhteisiä ratkaisuja $x \in \mathbb{Z}$. Jos x ja x' molemmat toteuttavat ko. kongruenssit, niin $x \equiv x' \pmod{mn}$.

Tod.: $\operatorname{syt}(m,n) = 1 \Rightarrow am + bn = 1$ eräillä $a, b \in \mathbb{Z}$ (tällaiset a ja b löytyvät esim. Euklideen algoritmilla). Olkoon $x = lma + knb \in \mathbb{Z}$. Silloin

$$\begin{aligned} x &\equiv knb \pmod m \\ &= k - kam \equiv k \pmod m \quad \text{ja} \\ x &\equiv lma \pmod n \\ &= l - lbn \equiv l \pmod n. \end{aligned}$$

Jos x ja x' molemmat toteuttavat nuo kongruenssit, niin $x - x' \equiv k - k = 0 \pmod m$ ja $x - x' \equiv l - l = 0 \pmod n$, ts. $m \mid (x - x')$ ja $n \mid (x - x')$.
Seur. lemma $\Rightarrow mn \mid (x - x')$. $\square$

Lemma: m ja n keskenään jaottomat, $m \mid k$ ja $n \mid k$
$\Rightarrow mn \mid k$.

Tod.: $\mathrm{syt}(m,n) = 1 \Rightarrow am + bn = 1$ eräillä $a, b \in \mathbb{Z}$.
$m \mid k, n \mid k \Rightarrow k = m'm = n'n$ eräillä $m', n' \in \mathbb{Z}$
$\Rightarrow k = 1 \cdot k = (am+bn) \cdot k$
$= am \cdot n'n + bn \cdot m'm$
$= mn \cdot (an + bm')$. □

Esim.: Ratkaise samanaikaiset kongruenssit
$x \equiv 2 \pmod 5$ ja $3x \equiv 5 \pmod{13}$.

Ratk. Koska $9 \cdot 3 = 27 = 1 + 2 \cdot 13 \equiv 1 \pmod{13}$,
on lauseen 8 nojalla

$$3x \equiv 5 \pmod{13} \iff x \equiv 9 \cdot 5 \pmod{13}$$
$$\iff x \equiv 45 \pmod{13}$$
$$\iff x \equiv 6 \pmod{13} \quad (45 = 6 + 3 \cdot 13).$$

Koska $8 \cdot 5 - 3 \cdot 13 = 1$, kiinal. jäännöslauseen tod.
$\Rightarrow$ kongruenssien $x \equiv 2 \pmod 5$ ja $x \equiv 6 \pmod{13}$
eräs yhteinen ratkaisu on

$$x = 6 \cdot 5 \cdot 8 + 2 \cdot 13 \cdot (-3) = 162.$$

Muut ratkaisut ovat $162 + s \cdot 65$, $s \in \mathbb{Z}$ $(6 = 5 \cdot 13)$,
joista nollan positiivinen on $162 - 2 \cdot 65 = 32$. □