Lukuteoria 1 10.2.2022

$m \in \mathbb{N} - \{0,1\}$. $a \in \mathbb{Z}$:n <u>kongruenssiluokka</u> mod m on

$$a + m\mathbb{Z} = \{ b \in \mathbb{Z} : b \equiv a \bmod m \} = \{ a + mk : k \in \mathbb{Z} \}.$$

Lause 1) $a \in a + m\mathbb{Z}$

2) $a \equiv b \bmod m \iff a + m\mathbb{Z} = b + m\mathbb{Z}$ } ti

3) pätee joko $a + m\mathbb{Z} = b + m\mathbb{Z}$ tai $(a + m\mathbb{Z}) \cap (b + m\mathbb{Z}) = \emptyset$.

Tod. 3) Ol. että $(a + m\mathbb{Z}) \cap (b + m\mathbb{Z}) \neq \emptyset$. Siis on $x \in (a + m\mathbb{Z}) \cap (b + m\mathbb{Z})$
$\Rightarrow a - b = ml - mk = m(l - k)$ $\quad \| \quad a + mk = b + ml$
$\Rightarrow a \equiv b \bmod m \overset{2)}{\Rightarrow} a + m\mathbb{Z} = b + m\mathbb{Z}$. $\square$ joillain $k, l \in \mathbb{Z}$.

1) $\Rightarrow \mathbb{Z} = \bigcup_{a \in \mathbb{Z}_{m-1}} a + m\mathbb{Z} = \bigcup_{r=0}^{m-1} r + m\mathbb{Z}$

Jakoyhtälö: $\forall a \in \mathbb{Z}$ on $q \in \mathbb{Z}$, $0 \le r \le m-1$:
$a = qm + r \iff a - r = qm \iff a \equiv r \bmod m$

$\Rightarrow$ $\mathbb{Z}$ on erillinen yhdiste m kongruenssiluokasta $r + m\mathbb{Z}$, $0 \le r \le m-1$

Fermat'n pieni lause. Olk. p alkuluku. Tällöin kaikille $a \in \mathbb{Z}$ pätee

$$a^p \equiv a \mod p.$$

Tod. Jos $p \mid a \Leftrightarrow a \equiv 0 \mod p$, niin $a^p \equiv 0^p = 0 \equiv a$. OK.

Ol. siten, että $p \nmid a$. Tällöin syt$(a,p) = 1$ koska p alkuluku.

Bézout: $\exists\, b, k \in \mathbb{Z}$: $ab + pk = 1 \Leftrightarrow ab \equiv 1 \mod p$.

Jos $ab_1 \equiv ab_2 \mod p$

L.5.4 $\Rightarrow$ $\underbrace{ba}_{=1} b_1 \equiv \underbrace{ba}_{=1} b_2 \mod p \Rightarrow b_1 \equiv b_2 \mod p$

Jokaisella $1 \le k \le p-1$ $\exists\, 1 \le x_k \le p-1 : ka \equiv x_k \mod p$.

Jos $k \ne l$, niin $x_k \ne x_l$

$\Rightarrow$ $a^{p-1}(p-1)! = (a\cdot 1)(a\cdot 2)\cdots(a\cdot p-1) \equiv x_1 \cdot x_2 \cdots x_{p-1} = 1\cdot 2\cdot 3\cdots(p-1) = (p-1)!$

$\equiv x_2$; $\equiv -a$; $x_1 = a$

nämä ovat kuvat $1, \dots, p-1$ eri järjestyksessä modulo p.

$\Rightarrow$ $a^{p-1}(p-1)! \equiv (p-1)! \mod p$.

5.5.8 $\Rightarrow$ $a^{p-1} \equiv 1 \mod p$ $\Rightarrow$ $a^p = a^{p-1}\cdot a \equiv a \mod p$. $\square$

Huom. Todistus osoitti myös että jos $b_1 a \equiv 1 \equiv b_2 a \mod p$, niin $b_1 \equiv b_2 \mod p$.

b_i:llä

$b_1 \equiv b_1 b_1 a \equiv b_2 b_1 a \equiv b_2$

($b_1 a \equiv 1$, $b_2 b_1 a = 1$)

Jos $\mathrm{syt}(m, c) = 1$ ja $ac \equiv bc \mod m$, niin $a \equiv b \mod m$.

Tod. Lause 5.7: Jos $ac \equiv bc \mod m$, niin $a \equiv b \mod \frac{m}{\mathrm{syt}(m,c)}$ ($= m$).

Esim. On yhdistetty ja luonnollinen luku $n \in \mathbb{Z}$ s.e. Fermat'n pienen lauseen lause ko $a^n \equiv a \mod n$ toteutuu jollekin $a \in \mathbb{Z}$:

$$2^{341} \equiv 2 \mod 341. \qquad 341 = 11 \cdot 31.$$

Fermat: $2^{10} \equiv 1 \mod 11$ (*) $\Rightarrow (2^{10})^{34} \equiv 1 \mod 11$

$2^{30} \equiv 1 \mod 31$ $\Rightarrow$ ei auta!

Kokeilemalla $2^5 = 32 \equiv 1 \mod 31 \Rightarrow 2^{10} \equiv 1 \mod 31$ (**)

(*) $\Leftrightarrow$ $11 \mid 2^{10}-1$ — Gaussin lemma $\Rightarrow$ s. 2.14

(**) $\Leftrightarrow$ $31 \mid 2^{10}-1$

$341 = 11 \cdot 31$ $\mid$ $2^{10}-1$ $\Leftrightarrow$ $2^{10} \equiv 1 \mod 341$

$\Rightarrow 2^{340} = (2^{10})^{34} \equiv 1^{34} = 1 \mod 341$

$\Rightarrow 2^{341} \equiv 2 \mod 341.$

341 on <u>valealkuluku</u> kannassa 2

Pienin yhteinen jaettava.

Määr. Olk. $a_1, \dots, a_N \in \mathbb{Z}-\{0\}$. c on lukujen a_j yhteinen jaettava, jos $a_j \mid c \ \forall\ 1 \le j \le N$. Lukujen $a_1, \dots, a_N$ pienin yhteinen jaettava $pyj(a_1, \dots, a_N)$ on niiden pienin positiivinen yhteinen jaettava.

Huom. $a_1 a_2 \cdots a_N$ on lukujen $a_1, \dots, a_N$ yhteinen jaettava.
$2 \cdot 5$ $2^2 \cdot 3$ $2^2 \cdot 3 \cdot 5$
$\|$ $\|$ $\|$

Esim $pyj(10,12) = 60$.

$10 \mid 10, 20, 30, 40, 50, 60, 70, \dots$

$12 \mid 12, 24, 36, 48, 60$

Lause 2.20 $a \neq 0 \neq b$.

$pyj(a,b) \mid c \iff a \mid c$ ja $b \mid c$

Tod. Jos $pyj(a,b) \mid c$ $\overset{\text{L.1.3(2)}}{\Longrightarrow}$ $a \mid c$ ja $b \mid c$.

$a \mid pyj(a,b)$

$b \mid pyj(a,b)$

Jakoyhtälö:

$$c = q\,\mathrm{pyj}(a,b) + r \qquad 0 \le r \le \mathrm{pyj}(a,b) - 1$$

Ol. että $a \mid c$ ja $b \mid c$.

$$\Rightarrow r = c - q\,\underbrace{\mathrm{pyj}(a,b)}_{\substack{a \mid \mathrm{pyj}(a,b) \\ b \mid}}$$

L.1.3 $\Rightarrow$ $a \mid r$ ja $b \mid r$, joten r on a:n ja b:n yht. jaettava.

mutta $0 \le r < \mathrm{pyj}(a,b) \Rightarrow \underline{r = 0}$ (pienin yht. jaettava)

$\Rightarrow \mathrm{pyj}(a,b) \mid c$. □

Lause 2.22

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

↑ Eukl. algoritmilla

↑ $= \dfrac{ab}{\mathrm{syt}(a,b)}$