Lukuteoria 1 17.2.2022

5.6. Osoita yhtälöiden $641 = 2^4 + 5^4 = 5 \cdot 2^7 + 1$ avulla, että $2^{32} \equiv -1 \mod 641$.

4.1. Osoita yhtälöiden $641 = 2^4 + 5^4 = 5 \cdot 2^7 + 1$ avulla, että $2^{32} = 641k - 1$ jollain $k \in \mathbb{N}$.[5]

Fermat'n luku $F^5 = 2^{2^5} + 1 = 2^{32} + 1$ ei ole alkuluku

$= 641\, k$

5.6:n ratkaisu. $641 = 2^4 + 5^4 \Rightarrow 5^4 \equiv -2^4 \mod 641$ (*)

$641 = 5 \cdot 2^7 + 1 \Rightarrow 5 \cdot 2^7 \equiv -1 \mod 641 \Rightarrow 5^4 \cdot 2^{28} \equiv 1 \mod 641$

L. 5.4 (3)

(*) $\Rightarrow -2^4 \cdot 2^{28} \equiv 1 \mod 641$

2^{32}

$\Rightarrow 2^{32} \equiv -1 \mod 641$

6 Lineaariset kongruenssiyhtälöt

Määr. $n \in \mathbb{N} - \{0,1\}$, $a, b \in \mathbb{Z}$

⊛ $ax \equiv b \mod n$ on lin. kongruenssiyhtälö.

Jos $x_0 \in \mathbb{Z}$, joka $ax_0 \equiv b \mod n$, niin x_0 on lin. kongruenssiyhtälön $ax \equiv b \mod n$ ratkaisu $(\mod n)$

Jos $x, y \in \mathbb{Z}$ ovat lin. kongr. yhtälön ⊛ ratkaisuja ja $x \equiv y \mod n$, niin x ja y ovat sama ratkaisu mod n.

Esim. 1) $\underbrace{2x}_{\text{parillinen}} \equiv 3 \mod \underbrace{4}_{\text{parillinen}}$
↑ pariton

$\text{syt}(2,4) \nmid 3$

⇒ Tällä kongruenssiyhtälöllä ei ole ratkaisua.

Jos x olisi ratkaisu, niin pitäisi olla $2x - 3 = 4k$ jollain $k \in \mathbb{Z}$

$\Leftrightarrow \underbrace{2x - 4k}_{\text{parillinen}} = 3$
↑ pariton.

2) $2x \equiv 6 \mod 12$ $\quad 2 = \text{syt}(2,12) \mid 6$.

Tällä on selvästi ainakin ratkaisu $\underline{\underline{x = 3}}$, koska $2 \cdot 3 = 6$ OK.

Lisäksi $2(3 + 12k) = 6 + 24k \equiv 6 \mod 12$.

Nämä ratkaisut ovat kongruenttejen mod 12 : $3 - (3 + 12k) = -12k$ $\frac{12}{2}$ "

Kokeilemalla : $2 \cdot 9 = 18 = 6 + 12 \equiv 6 \mod 12$. Siis myös $\underline{\underline{x = 9 = 3 + 6}}$

(ja $x = 9 + 12l$, $l \in \mathbb{Z}$) on kongr. yhtälön ratkaisu. (L. 6.4 kaikki ratkaisut löydetty)

<u>Lemma</u> Jos $c \in \mathbb{Z}$ on kongr. yhtälön $ax \equiv b \mod m$ ratkaisu, niin $c + mk$, $k \in \mathbb{Z}$, on ratkaisu.

<u>Tod.</u> $c + mk \equiv c \mod m$. L. 5.4 : $\underline{a(c + mk) \equiv ac \mod m}$
" b

Voidaan myös sanoa, että kongruenssiluokka $c + m\mathbb{Z}$ on kongr. yhtälön $ax \equiv b \mod m$ ratkaisu, jos c on sen ratkaisu.

(3)

Lause 6.4 Olk. $m \in \mathbb{N} - \{0,1\}$, $a, b \in \mathbb{Z}$

1) Jos $\operatorname{syt}(a,m) \nmid b$, niin kongr. yhtälöllä $ax \equiv b \bmod m$ ei ole ratkaisuja.

2) Jos $\operatorname{syt}(a,m) \mid b$, niin yhtälöllä $ax \equiv b \bmod m$ $\operatorname{syt}(a,m)$ ratkaisua mod m

Jos x_0 on ratkaisu, niin kaikki ratkaisut mod m ovat

$$x_0 + j \underbrace{\frac{m}{\operatorname{syt}(a,m)}}_{\in \mathbb{Z}}, \quad j \in \underbrace{\{0, 1, \ldots, \operatorname{syt}(a,m) - 1\}}_{\operatorname{syt}(a,m) \text{ kpl.}}$$

Tod. 1) Jos $x \in \mathbb{Z}$ on yhtälön $ax \equiv b \bmod m$ ratkaisu, niin

$ax - b = km$ jollain $k \in \mathbb{Z}$

$\hookrightarrow ax + km = b$ L. 2.7: yhtälöllä $\circledast$ ei ole ratkaisua.

$\circledast$ Siis kongr. yhtälöllä $ax \equiv b \bmod m$ ei ole ratkaisuja.

2) Ol. että $\mathrm{syt}(a,m) \mid b$. Bézout:

Seuraus 2.5 (Bézout'n yhtälö). *Olkoot $a, b \in \mathbb{Z}$, $a \neq 0$. Tällöin*

$$\mathrm{syt}(a,b) = xa + yb$$

joillain $x, y \in \mathbb{Z}$.

$\Rightarrow b = a k_0 + m l_0$ joillain $k_0, l_0 \in \mathbb{Z}$

$\hookrightarrow a k_0 - b = -m l_0$

$\Rightarrow a k_0 \equiv b \bmod m$ siis k_0 on ratkaisu.

Muut ratkaisut:

$$a\left(k_0 + j\frac{m}{\mathrm{syt}(a,m)}\right) = ak_0 + m \cdot j \cdot \underbrace{\frac{a}{\mathrm{syt}(a,m)}}_{\in \mathbb{Z}} \equiv ak_0 \equiv b \bmod m$$

tämä on ratkaisu!

Huom $\left(k_0 + j_1\frac{m}{\mathrm{syt}(a,m)}\right) - \left(k_0 + j_2\frac{m}{\mathrm{syt}(a,m)}\right) = (j_1 - j_2)\frac{m}{\mathrm{syt}(a,m)}$

$= n\,m \iff \mathrm{syt}(a,m) \mid (j_1 - j_2)$

$\iff k_0 + j_1\frac{m}{\mathrm{syt}(a,m)} \equiv k_0 + j_2\frac{m}{\mathrm{syt}(a,m)}$

$\iff \mathrm{syt}(a,m) \mid j_1 - j_2 \Rightarrow$ väitteen ratkaisut ovat eri ratkaisuja mod m.

Siis ratkaisu jo on ainakin syt (a,m) kpl, ne, jotka on luetelty vaihtoehdoissa. Os. vielä, että muita ratkaisuja ei ole!

Olk. x, y yhtälön $ax + my = b$ ratkaisu ($ax \equiv b \bmod m$)

Edellä oli ratk. $ak_0 + ml_0 = b$.

$$a(x-k_0) + m(y-l_0) = \underbrace{(ax+my)}_{=b} - \underbrace{(ak_0+ml_0)}_{=b} = 0$$

$$\Leftrightarrow a(x-k_0) = -m(y-l_0)$$

$$\Rightarrow \frac{a}{\operatorname{syt}(a,m)}(x-k_0) = -\frac{m}{\operatorname{syt}(a,m)}(y-l_0) \quad \Big| \text{ S. 2.12 } \operatorname{syt}\left(\frac{a}{\operatorname{syt}(a,m)}, \frac{m}{\operatorname{syt}(a,m)}\right) = 1$$

$$\frac{m}{\operatorname{syt}(a,m)} \Big| \frac{a}{\operatorname{syt}(a,m)}(x-k_0) \quad \Big| \text{ Gaussin lemma 5.2.14}$$

$$\Rightarrow \frac{m}{\operatorname{syt}(a,m)} \Big| x-k_0 \Rightarrow x-k_0 = i\frac{m}{\operatorname{syt}(a,m)} \Rightarrow x = k_0 + i\frac{m}{\operatorname{syt}(a,m)}$$

jollain $i \in \mathbb{Z}$ □

Seuraus Jos $\mathrm{syt}(a,m) = 1$, niin kongr. yhtälöllä $ax \equiv b \bmod m$ on täsmälleen 1 ratkaisu mod m.

Seuraa L. 6.4: yhtälöllä on 1 ratkaisu mod 12

Esim. 1) $7x \equiv 3 \bmod 12$. $\mathrm{syt}(7,12) = 1$ (7 alkuluku).

Ratkaistaan yhtälö $7x + 12y = 1 = \mathrm{syt}(7,12)$

Saadaan $x, y \rightsquigarrow (3x, 3y)$ on yhtälön $7x + 12y = 3$ ratkaisu

$\rightsquigarrow$ x on kongr. yhtälön $7x \equiv 3 \bmod 12$ ratkaisu.

Eukleideen algoritmi: $12 = 1 \cdot 7 + 5 \iff 5 = 12 - 1 \cdot 7$

$7 = 1 \cdot 5 + 2 \iff 2 = 7 - 1 \cdot 5$

$5 = 2 \cdot 2 + 1$

Permuteetaan: $1 = 5 - 2 \cdot 2 = 5 - 2(7 - 1 \cdot 5) = 3 \cdot 5 - 2 \cdot 7$

$= 3(12 - 7) - 2 \cdot 7 = 3 \cdot 12 - 5 \cdot 7$

$x = -5$ on yhtälön $7x \equiv 1 \bmod 12$ ratkaisu ratk.

$\Rightarrow 3(-5) = -15 \equiv -3 \equiv 9 \bmod 12$ on yhtälön $7x \equiv 3 \bmod 12$