Harjoitukset 5 Ratkaisut **Lukuteoria**
tiistai 18.10.2011 16.00-17.30 MaD-302

1. ...

Luku 123456789 on jaollinen jopa 9:llä, , koska 1+2+...9=45 ja $4+5=9$.
Luku 123456789 ei ole jaollinen 11:llä, , koska $11 \not| 1-2+\cdots+9=5$.
Luku 476271 ei ole alkuluku, koska 4+7+6+2+7+1=27 on jaollinen kolmella.

2. *Jaollisuuslauseet 4:llä ja 8:lla.*

(i) 4:llä: Kymmenen potenssien jakojäännökset neljällä (eli kympin potenssit modulo 4) ovat $1 \equiv 1, 10 \equiv 2, 100 \equiv 2^2 = 4 \equiv 0$ ja siis loputkin nollia. Siis desimaaliluvut $a_n a_{n-1} \dots a_1 a_0$ ja $a_1 a_0$ sekä luku $2a_1 + a_0$ ovat yhtä aikaa jaolliset nelosella, esim $222222 \equiv 22$ ei ole, eikä myöskään $2 \cdot 2 + 2 = 4$ ole, mutta $600560 \equiv 60$ on, samoin $2 \cdot 6 + 0$. Lopuksi: 3416 on, koska 16 on.

(ii) 8:lla: Kymmenen potenssien jakojäännökset 8:lla (eli kympin potenssit modulo 8) ovat $1 \equiv 1, 10 \equiv 2, 100 \equiv 2^2 = 4, 1000 \equiv 2^3 = 8 \equiv 0$ ja siis loputkin nollia. Siis desimaaliluvut $a_n a_{n-1} \dots a_1 a_0$ ja $a_2 a_1 a_0$ sekä $4 \cdot a_2 + 2 \cdot a_1 + a_0$ ovat yhtä aikaa jaolliset 8:lla. Esim $222222 \equiv 222$ ei ole, eihän $4 \cdot 2 + 2 \cdot 2 + 2 = 8 + 4 + 6$ ole, mutta $600560 \equiv 560$ on, sillä $4 \cdot 5 + 2 \cdot 6 + 0 = 20 + 12 = 32$ on jaollinen 8:lla (voi lopuksi soveltaa testiä vielä kerran: $0 \cdot 2 + 3 \cdot 2 + 2 = 8$ on jaollinen. Lopuksi: 3416 on, koska 416 on, koska $4 \cdot 4 + 2 \cdot 1 + 6 = 16 + 2 + 6 = 24$ on jaollinen 8:lla.

3. *Algebrasta tiedetään, että*

Määr: *(Äärellisen)* ryhmän kertaluku *on sen alkioiden lukumäärä.*
Määr: *Ryhmän* G alkion a kertaluku *on* $\min\{n \in \mathbb{N} \mid a^n = 1\}$ *(, joka on itse asiassa alkion* a *virittämän aliryhmän* $\langle a \rangle$ *alkioiden lukumäärä.)*
Lagrangen lause: *Ryhmän alkion kertaluku jakaa ryhmän kertaluvun.*

Todistetaan Eulerin lause.

Eulerin funktion määritelmän mukaan $\varphi(n)$ on ryhmän $\mathbb{Z}_n^*$ kertaluku, joten Lagrangen lauseen mukaan alkion $a \in \mathbb{Z}_n^*$ kertaluku N jakaa luvun $\varphi(n)$, ts. $\varphi(n) = Nk$ jollekin $k \in \mathbb{N}$. Alkion kertaluvun määritelmän mukaan $a^N = 1 \in \mathbb{Z}_n^*$, joten

$$a^{\varphi(n)} = a^{Nk} = (a^N)^k = 1^k = 1 \in \mathbb{Z}_n^*. \quad \square$$

4. *Ratkaise lineaariset kongruenssiyhtälöt (a) ja (b) ja selvitä kongruenssiyhtälöiden (c) ja (d) ratkaisujen lukumäärä.*

(a) $3x \equiv 5 \pmod 7$.
Koska $(3, 7) = 1$, niin ratkaisu on 1-käsitteinen ja saadaan kertomalla puolittain 3:n käänteisellä (mod 7), joka on 5.(kokeilin vaihtoetoja 2,3,4,5,6, huomsin heti, että $3 \cdot 2 = 6 = -1$, joten $3 \cdot 2 \cdot 3 \cdot 2 = 1$ eli $1 = 3 \cdot (2 \cdot 3 \cdot 2) = 3 \cdot 12 = 3 \cdot 5$, ja todella: $3 \cdot 5 = 15 = 1$.) Siis $x = 5^2 = 25 = 4 \in \mathbb{Z}_7$.

(b) $6x \equiv 5 \pmod{12}$.
Koska $(6, 12) = 6 \not| 5$, niin ratkaisuja ei ole (Lause 2.27).

(c) $943x \equiv 381 \pmod{2576}$
Koska $(943, 2576) = 23$ (<-Eukleideen algoritmi taskulaskimella.) ja $23 \not| 381$, niin ratkaisua ei ole

(d) $1375x \equiv 242 \pmod{5625}$ Koska $(1375, 5625) = 11$ ja $242 = 22 \cdot 11$, niin ratkaisuja on 11 kpl.

5. *Ratkaise* $6x \equiv 4 \pmod{10}$.

Koska $(6, 10) = 2$ ja $2 \mid 4$, niin ratkaisuja on 2 kpl. Ne löydetään 3 menetelmällä:

(1) kokeilemalla: $6 \cdot 0 = 0 \not\equiv 4 \pmod{10}$
$6 \cdot 1 = 6 \not\equiv 4 \pmod{10}$
$6 \cdot 2 = 12 \equiv 2 \not\equiv 4 \pmod{10}$
$6 \cdot 3 = 18 \not\equiv 4 \pmod{10}$
$6 \cdot 4 = 24 \equiv 4 \pmod{10}$ OK!
$6 \cdot 5 = 30 \not\equiv 4 \pmod{10}$
$6 \cdot 6 = 36 \not\equiv 4 \pmod{10}$
$6 \cdot 7 = 42 \not\equiv 4 \pmod{10}$
$6 \cdot 8 = 48 \not\equiv 4 \pmod{10}$
$6 \cdot 9 = 54 \equiv 4 \pmod{10}$ OK!
Ja todella 9=4+10/2, kuten teoria edellyttääkin.

(2) Eulerilla: Jaetaan ensin pois $(6, 10)$ eli 2 ja siirrytään tarkastelemaan kongruenssia $3x \equiv 2 \pmod{5}$.
$\varphi(5) = 4$, joten $x \equiv 3^{varphi(10)-1} = 3^3 = 9 \equiv 4$. Toinen ratkaisu (eli 9) saadaan lisäämällä 10/2 eli 5.

(3) Eukleideella luennon/monisteen ohjeen mukaan: Jaetaan taas ensin pois $(6, 10)$ eli 2 ja siirrytään tarkastelemaan kongruenssia $3x \equiv 2 \pmod{5}$. Etsitään Eukleideen algoritmilla luvut y ja z siten, että $3y + 5z = 1$:

$5 = 3 + 2, \quad 3 = 2 + 1,$ siis

$1 = 3 - 2 = 3 - (5 - 3) = 2 \cdot 3 - 1 \cdot 5,$ joten kelpaa $y = 2$, $x = -1$.

mistä näkyy, että $3y \equiv 1 \pmod{5}$ eli $3 \cdot 2 \equiv 1 \pmod{5}$, mistä päätellään, että $3 \cdot 2 \cdot 2 \equiv 2 \pmod{5}$, siis $x = 4$ kelpaa. Toinen ratkaisu (eli 9) saadaan jälleen lisäämällä 10/2 eli 5.

On syytä panna merkille, että **lineaarisen kongruenssin** $ax \equiv 1 \pmod{n}$ **ratkaiseminen on sama tehtävä kuin käänteisalkion** $a^{-1} \in \mathbb{Z}_n$ **etsiminen.** (Monisteessa käänteistä on merkitty a'.)

6. *Kalle ei muista, montako porttia pujotteluradalla on, mutta hän muistaa, että jos porttien määrä jaetaan kahdella, kolmella, tai seitsemällä.*

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 0 \pmod{7} \end{cases}$$

Ratkaisu on helppo keksiä suoraankin kokeilemalla 7:llä jaollisia lukuja, mutta esitetaään teorian (kertauksen) mukainen ratkaisu:

Huomataan aluksi, että 2, 3 ja 7 ovat parittain suhteellisia alkulukuja (itse asiassa jopa eri alkulukuja), OK! Tulos saadaan lukuna $x = 1 \cdot y + 2 \cdot z + 0 \cdot w$, missä luvut y, z, w toteuttavat seuraavat helpommat kongruenssiryhmät, jotka ratkaistaan ensin:

$$\begin{cases} y \equiv 1 \pmod{2} \\ y \equiv 0 \pmod{3} \\ y \equiv 0 \pmod{7} \end{cases}, \quad \begin{cases} z \equiv 0 \pmod{2} \\ z \equiv 1 \pmod{3} \\ z \equiv 0 \pmod{7} \end{cases} \text{ ja } \quad \begin{cases} w \equiv 0 \pmod{2} \\ w \equiv 0 \pmod{3} \\ w \equiv 1 \pmod{7} \end{cases}$$

Olkoon

$$n_1 = 2,\ n_2 = 3,\ n_3 = 7,\ N = n_1 n_2 n_3 = 42,$$

ja

$$N_1 = N/n_1 = n_2 n_3 = 21,\ N_2 = N/n_2 = n_1 n_3 = 14,\ \text{ja}\ N_3 = N/n_3 = n_1 n_2 = 6.$$

Teorian mukaan ratkaisu on yksikäsitteinen $\pmod N$, joten riittäälöytää yksi ratkaisu $x \in \mathbb{Z}$. Se löydetään näin: Kongruenssiryhmä $\begin{cases} y \equiv 1 \pmod 2 \\ y \equiv 0 \pmod 3 \\ y \equiv 0 \pmod 7 \end{cases}$ merkitsee, että on löydettävä **luku** y, joka on jaollinen 3:lla ja 7:lla, siis muotoa $y = N_1 k = 21k$ ja jolle $y \equiv 1 \pmod 2$. On siis ratkaistava kongruenssi $y = 21k \equiv 1 \pmod 2$ eli löydettävä luvun $21 = N_1$ käänteisalkio $k = N_1' \in \mathbb{Z}_2$. Se on tietenkin 1, onhan $N_1 = 21 \equiv 1 \pmod 2$. Siis $y = 21 \cdot 1 = 21$, minkä heti kokeillessaan huomaa todella toteuttavan ao. kongruenssiryhmän.

Vastaavasti saadaan z:n kongruenssiryhmästä $\begin{cases} z \equiv 0 \pmod 2 \\ z \equiv 1 \pmod 3 \\ z \equiv 0 \pmod 7 \end{cases}$, että $z = 14N_2'$, missä $14N_2' \equiv 1 \pmod 3$, eli (esim.) $N_2' = 2$, josta $z = 28$ mikä toteuttaakin ao. kongruenssiryhmän.

Kolmannen kongruenssiryhmän ratkaisemiselta vältytään, koska alkuperäisessä tehtävässä kolmas jakojäännös on 0 ja ratkaisu siis $x = y + 2x + 0w = 21 + 2 \cdot 28 = 77$. Koska $N = 42$, niin 35=77-42 on pienin positiivinen ratakaisu ja voi lopuksi laskuvirheiden varalta että 35 toteuttaa alkuperäisen kongruenssiryhmän. $\begin{cases} 7 \equiv 1 \pmod 2 \\ 7 \equiv 2 \pmod 3 \\ 7 \equiv 0 \pmod 7 \end{cases}$

Muistaen alkuperäien tehtävän voisi arvata, että Kallen portteja on 35 kpl (ei kai sentään esim 77 eikä 112 kpl?).

7. *Ratkaisen kongruenssiryhmät Kallen opeilla.*

Koska käänteiset N_j' **lasketaan eri modulien** n_j **suhteen**, on niitä seuraavassa merkitty $(N_j)_j^{-1}$, mikä ei ole vakiintunut käytäntö, mutta helpottanee ajattelaua aluksi.

a) $\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 5 \pmod 7 \\ x \equiv 7 \pmod{12} \end{cases}$ Siis $x = 2y + 5z + 7w$,

$y = (7 \cdot 12) \cdot (7 \cdot 12)_5^{-1} = 84 \cdot (84)_5^{-1} = 84 \cdot (4)_5^{-1} = 84 \cdot 4 = 336.$

(Sama fixummin:

$y = (7 \cdot 12) \cdot (7 \cdot 12)_5^{-1} = 84 \cdot (2 \cdot 2)_5^{-1} = 84 \cdot (4)_5^{-1} = 84 \cdot 4 = 336.$

$z = (5 \cdot 12) \cdot (5 \cdot 12)_7^{-1} = 60 \cdot (60)_7^{-1} = 60 \cdot (4)_7^{-1} = 60 \cdot 2 = 120.$

$w = (5 \cdot 7) \cdot (5 \cdot 7)_{12}^{-1} = 35 \cdot (35)_{12}^{-1} \cdot 2 = 35 \cdot (-1)_{12}^{-1} = 35 \cdot 11 = 385.$

$x = 2 \cdot 336 + 5 \cdot 120 + 7 \cdot 385 = 3967 \equiv \mathbf{187} \pmod{5 \cdot 7 \cdot 12 = 420}$

b) $\begin{cases} x \equiv 2 \pmod 6 \\ x \equiv 5 \pmod 7 \\ x \equiv 7 \pmod{15} \end{cases}$ Tässä on ongelma: $(6, 15) \neq 1$. Hädän hetkellä improvisoidaan hieman. Ensimmäinen kongruenssi merkitseee, että $x - 2$ on jaollinen 6:lla, siis sekä 2:lla että 3:lla. Näin kongruenssiryhmä saa muodon

b') $\begin{cases} x \equiv 0 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 5 \pmod 7 \\ x \equiv 7 \pmod{15} \end{cases}$

Vastaavasti alin kongruenssi $x \equiv 7 \pmod{15}$ jakautuu pariksi $\begin{cases} x \equiv 7 \equiv 1 \pmod 3 \\ x \equiv 7 \equiv 2 \pmod 5 \end{cases}$
Kongruenssiryhmällä ei ei ole ratkaisua, koska etsitty luku olisi parillinen (1. kongruenssi) ja samalla pariton (alin kongruenssi).

c) $\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 5 \pmod 7 \\ x \equiv 8 \pmod{12} \end{cases}$

Siis $x = 2y + 5z + 8w$, missä x, y ja z ovat samat kuin a)-kohdassa, siis $y = 336$, $z = 120$ ja $w = 385$. Riittää siis lisätä a):n ratkaisuun yhden kerran w ja saadaan $x = 187 + 385 = 572 \equiv \mathbf{152} \pmod{420}$. (Kokeilin: toimii)

d) $\begin{cases} x \equiv 3 \pmod 9 \\ x \equiv 6 \pmod{10} \\ x \equiv 9 \pmod{11} \end{cases}$ Siis $x = 3y + 6z + 9w, \quad N = 990.$

$y = (10 \cdot 11) \cdot (10 \cdot 11)^{-1}{}_9 = 110 \cdot (1 \cdot 2)_9^{-1} = 110 \cdot (2)_9^{-1} = 110 \cdot 5 = 550.$
$z = (9 \cdot 11) \cdot (9 \cdot 11)_{10}^{-1} = 99 \cdot (-1 \cdot 1)_{10}^{-1} = 99 \cdot 9 = 891.$
$w = (9 \cdot 10) \cdot (9 \cdot 10)_{11}^{-1} = 90 \cdot (2)_{11}^{-1} = 90 \cdot 6 = 540.$
$x = 3 \cdot 550 + 6 \cdot 891 + 9 \cdot 540 = 11856 \equiv \mathbf{966} \pmod{9 \cdot 10 \cdot 11 = 990}.$

8. *(Virhe tehtävässä korjattu.) Olkoot p ja q eri alkulukuja. Osoita, että*

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

Fermat'n pienen lauseen mukaan

$$p^{q-1} \equiv 1 \pmod q, \text{ joten } p^{q-1} + q^{p-1} \equiv 1 \pmod q.$$
$$\text{Vastaavasti } q^{p-1} \equiv 1 \pmod p, \text{ joten } p^{q-1} + q^{p-1} \equiv 1 \pmod p,$$
$$\text{joten, koska } (p, q) = 1, \; p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

9. *Olkoon p alkuluku.*

(a) $(a + b)^p \overset{Fermat}{\equiv} a + b \overset{Fermat}{\equiv} a^p + b^p \pmod p$.
(b) $(a+b)^p = \sum_{k=1}^{p} \binom{p}{k} a^k b^{m-k} \equiv a^p + b^p \pmod p$, *(Koska $p \mid \binom{p}{k}$, kun $1 < k < p$.)*
(c) *Todistetaan Fermat'n kaava induktiolla a:n suhteen. Alku:* $1^p = 1 \equiv 1 \pmod p$
Askel: $(a + 1)^p \overset{2)}{\equiv} a^p + 1^p = a^p + 1 \overset{Ind.ol}{\equiv} a + 1.$