Harjoitukset 7 Ratkaisut **Lukuteoria**
tiistai 1.11.2011 16.00-17.30 MaD-302

1. *Osoita, että kaikille parittomille alkuluvuille p pätee*
   a) $(p-2)! \equiv 1 \pmod{p}$.
   b) $2 \cdot (p-3)! \equiv 1 \pmod{p}$.

Vihje: Ryhmässä kaikki alkiot ovat kääntyviä. Millä alkioilla on $a \neq a^{-1} \in Z_p^*$? Mikä on muiden tulo?

Ratkaisu.

a) Ryhmässä Z_p^* on kaikkien alkioiden tulo $(p-1)!$. Ykkösen voi jättää pois ja alkio $p-1$ eli -1 puuttuu tehtävän tulosta. 1 ja -1 ovat ne alkiot, joiden käänteinen on alkio itse, eli yhtälön $x^2 = x$ molemmat ratkaisut. Muut alkiot $a \in \mathbb{Z}_p^*$ ovat parittain toistensa käänteisiä, joten niiden tulo on 1. Siis $(p-2)! \equiv 1 \pmod{p}$. Tämä oli kertaustehtävä! Vrt. Wilsonin lausen todistus! Voit ratkaista tehtävän myös käyttämällä Wilsonin lausetta:

$$(p-1)! \equiv -1 \pmod{p} \iff p \in \mathbb{P}.$$

b) Ryhmässä Z_p^* on siis

$$2 \cdot (p-3)! = 2\frac{(p-2)!}{p-2} = 2\frac{(p-2)!}{-2} = -(p-2)! = -1.$$

2. *Kaikille parittomille alkuluvuille p pätee*

$$1^2 \cdot 3^2 \cdot 5^2 \cdot \cdots \cdot (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$$

Ratkaisu:

$$\begin{aligned}
&1^2 \cdot 3^2 \cdot 5^2 \cdot \cdots \cdot (p-2)^2 \equiv (1 \cdot 3 \cdot 5 \cdot \cdots \cdot (p-2))^2 \\
&\equiv \big(1 \cdot 3 \ldots (p-2)\big) \cdot \big((p-2)(p-4)\ldots(p-(p-1))\big) \\
&\equiv 1 \cdot 3 \ldots (p-2) \cdot (-2)(-4)\ldots(-(p-1)) \\
&\equiv (-1)^{\frac{p-1}{2}}(p-1)! \equiv (-1)^{\frac{p-1}{2}} \cdot (-1) = 1(-1)^{\frac{p+1}{2}} \pmod{p}.
\end{aligned}$$

3. *Määrää kaikki neliönjäännökset* (mod 23). *Kirjoita näkyviin niiden itseisarvoltaan pienimmät edustajat. Minkä (todistetun) ilmiön huomaat?*

Ratkaisu: Korottele neliöön. Tulos: 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18. eli 1, 2, 3, 4, 6, 8, 9, -11, -10, -7, -5. Itseisarvot ovat luvut 1,2,... $\frac{23-1}{2} = 11$.

4. *Tutki Eulerin kriteerillä, onko 2 neliönjäännös* (mod 17). *Entä 5?*

Ratkaisu: Lasketaan Legendren symboli $\left(\frac{2}{17}\right)$. Eulerin kriteeri sanoo, että jos p on pariton alkuluku, niin

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Tässä $p = 17$ ja $a = 2$, joten saadaan

$$\left(\frac{2}{17}\right) \equiv 2^8 \equiv 1 \pmod{17}.$$

Siis 2 on neliönjäännös $\pmod{17}$.

Vastaavasti

$$\left(\frac{5}{17}\right) \equiv 5^8 \equiv -1 \pmod{17}.$$

Siis 5 ei ole neliönjäännös $\pmod{17}$.

5. *Kuinka monta (epäkongruenttia, tietenkin) ratkaisua on kongruenssilla* $x^2 \equiv 2$ a) $\pmod{17}$, b) $\pmod{17^2}$, *(Entä* c) $\pmod{17^{100}}$, *tai* d $\pmod{10}$*?) Vihje: 2,2,(2,0).*

Ratkaisu

a) $x^2 \equiv 2 \pmod{17}$ on 2. asteen yhtälö kunnssa, joten sillä on enintään 2 ratkaisua, ja ne ovat olemassa, koska 2 on neliönjäännös $\pmod{17}$, kuten edellä todettiin laskemalla $\left(\frac{2}{17}\right)$. Ratkaisut ovat ± 6 eli 6 ja 11.

b) $x^2 \equiv 2 \pmod{17^2}$ palautuu edelliseen huomaamalla, että

$$x^2 \equiv 2 \pmod{17^2} \implies x^2 \equiv 2 \pmod{17},$$

joten ratkaisuehdokkaat ovat a)-kohdan mukaan joukossa $\{6 + n \cdot 17 \mid n \in 0, 1, \ldots 16\}$ tai $\{-6 + n \cdot 17 \mid n \in 0, 1, \ldots 16\}$. Kummankin joukon luvut ovat epäkongruentteja keskenään $\pmod{17^2}$, joten ratkaisuja on enintään 2 kpl. Kummastakin löytyy ratkaisu, minkä huomaa ratkaisemalla tarvittavan kongruenssin:

$$\begin{aligned}
(6 + n \cdot 17)^2 &\equiv 2 \pmod{17^2} \\
36 + 2 \cdot n \cdot 17 + n^2 17^2 &\equiv 2 \pmod{17^2} \\
(2 + 2 \cdot 17) + 2 \cdot n \cdot 17 + 0 &\equiv 2 \pmod{17^2} \\
2 \cdot 17 + 2 \cdot n \cdot 17 &\equiv 0 \pmod{17^2} \\
2 + 2 \cdot n &\equiv 0 \pmod{17}
\end{aligned}$$

Tällä on yksikäsitteinen ratkaisu (tietenkin se on -1 eli 16, mutta voi muistaa, että lineaarisen kongruenssin ratkaisu on yleensäkin yksikäsitteinen, kun moduli on alkuluku, kuten 17 on.) Vastaavasti toinen.

Lisäkysymys c) on vastaavanlainen. $x^2 \equiv 2 \pmod{17^{100}}$ palautuu edelliseen huomaamalla, että

$$x^2 \equiv 2 \pmod{17^{100}} \implies x^2 \equiv 2 \pmod{17^b} \quad \forall 1 \leq b \leq 100,$$

joten b)-kohdan päättelyä voi soveltaa induktiolla ja päätyä siihen, että ratkaisuja on kussakin modulin potenssissa 2 epäkongruenttia.

6. *Onko alkiolla 2 neliöjuuri kunnassa* $\mathbb{Z}_{29}$*, kunnassa* $\mathbb{Z}_{31}$*,* $\mathbb{Z}_{97}$*,* $\mathbb{Z}_{101}$ *tai* $\mathbb{Z}_{111}$*?*

Käytetään resiprookkilain 2. täydennyslausetta 3.1, jonka mukaan

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, \text{ jos } p = 8n \pm 1 \\ -1, \text{ jos } p = 8n \pm 3. \end{cases}$$

Ratkaisu $\left(\frac{2}{29}\right) = -1$, koska $29 = 4 \cdot 8 - 3$, vastaavasti $\left(\frac{2}{31}\right) = 1$, $\left(\frac{2}{97}\right) = 1$, $\left(\frac{2}{101}\right) = -1$, $\left(\frac{2}{111}\right) = -1$.

7. Ratkaisu

a) $$\left(\frac{61}{31}\right) = \left(\frac{61-31}{31}\right) = \left(\frac{30}{31}\right) = \left(\frac{2}{31}\right)\left(\frac{3}{31}\right)\left(\frac{5}{31}\right)$$
$$= \left(\frac{2}{32-1}\right)\left(\frac{31}{3}\right)(-1)^{\frac{31-1}{2}\frac{3-1}{2}}\left(\frac{31}{5}\right)(-1)^{\frac{31-1}{2}\frac{5-1}{2}}$$
$$= \left(\frac{2}{32-1}\right)\left(\frac{1}{3}\right)(-1)^{15\cdot 1}\left(\frac{1}{5}\right)(-1)^{15\cdot 2} = 1\cdot 1\cdot(-1)\cdot 1\cdot 1 = -1.$$

b) $$\left(\frac{33}{31}\right) = \left(\frac{33-31}{31}\right) = \left(\frac{2}{31}\right) = 1.$$

c) $$\left(\frac{29}{31}\right) = \left(\frac{31}{29}\right)(-1)^{\frac{31-1}{2}\frac{29-1}{2}} = -\left(\frac{31}{29}\right) = -\left(\frac{2}{32-3}\right) = -1.$$

d) $$\left(\frac{8}{31}\right) = \left(\frac{2\cdot 2\cdot 2}{31}\right) = \left(\frac{2}{31}\right)^3 = (1)^3 = 1.$$

e) $$\left(\frac{128}{821}\right) = \left(\frac{2^7}{821}\right) = (\left(\frac{2}{821}\right))^7 = \left(\frac{2}{821}\right) = -1.$$

8. Ratkaisu

a) Gaussin lemmalla, alkuperäinen versio:

$$\left(\frac{3}{17}\right) = (-1)^s,$$

missä $s = \#\{k\cdot 3 = r_k\epsilon_k \mid 1 \le k \le \frac{16}{2},\ \epsilon_k < 0\}$. Lasketaan s:

$$\begin{aligned} 3 &\equiv 3 \pmod{17}\\ 6 &\equiv 6 \pmod{17}\\ 9 &\equiv -8 \pmod{17}\\ 12 &\equiv -5 \pmod{17}\\ 15 &\equiv -2 \pmod{17}\\ 18 &\equiv 1 \pmod{17}\\ 21 &\equiv 4 \pmod{17}\\ 24 &\equiv 7 \pmod{17}. \end{aligned}$$

Negatiivisia on 3 kpl, siis pariton määrä, joten 3 on epäjäännös (mod 17). (Virheiden välttämiseksi voi vielä tarkastaa, että itseisarvoina todella esiintyvät kaikki luvut $1\ldots 8$.)

a') Gaussin lemmalla, analyyttinen versio 3.13.:

$$\left(\frac{3}{17}\right) = (-1)^T,$$

missä $T = \sum_{x=1}^{(17-1)/2}\lfloor\frac{2\cdot 3\cdot x}{17}\rfloor$. Lasketaan $T = \sum_{x=1}^{8}\lfloor\frac{6\cdot x}{17}\rfloor$:

$$T = \lfloor\frac{6}{17}\rfloor+\lfloor\frac{12}{17}\rfloor+\lfloor\frac{18}{17}\rfloor+\lfloor\frac{24}{17}\rfloor+\lfloor\frac{30}{17}\rfloor+\lfloor\frac{36}{17}\rfloor+\lfloor\frac{42}{17}\rfloor+\lfloor\frac{48}{17}\rfloor+ = 2\cdot 0+3\cdot 1+3\cdot 2 = 11,$$

siis pariton, joten 3 on epäjäännös $\pmod{17}$.

b) Eulerin ehdolla:

$$\left(\frac{3}{17}\right) \equiv 3^{\frac{17-1}{2}} = 3^8 = 81^2 \equiv 13^2 \equiv 169 \equiv -1 \pmod{17}.$$

c) Resiprookkilauseella: $\left(\frac{3}{17}\right) \equiv \left(\frac{17}{3}\right)(-1)^{8\cdot 1} \equiv \left(\frac{17}{3}\right) = \left(\frac{17-5\cdot 3}{3}\right) = \left(\frac{2}{3}\right) = -1$

9. *Olkoon p pariton alkuluku ja $ab \equiv 1 \pmod{p}$. Osoita, että jos kongruenssilla $x^2 \equiv a \pmod{p}$ on ratkaisu, niin myös kongruenssilla $x^2 \equiv b \pmod{p}$ on ratkaisu.*

Ratkaisu: Kunnassa $\mathbb{Z}_p$ on alkiolla $x \neq 0$ olemassa käänteisalkio x^{-1}. Jos $x^2 \equiv a \pmod{p}$, niin $(x^{-1})^2 = (x^2)^{-1} \equiv a^{-1} \equiv b \pmod{p}$.