Lukuteorian alkeet
viidensien harjoitusten ratkaisuita

1. 25.1.2013 löytyi 48. Mersennen alkuluku, joka on

$$2^{57885161} - 1.$$

Mikä on luvun 2 kertaluku tässä modulossa? Entä lukujen 4 ja 8?

Ratkaisu. Merkitään $p = 2^{57885161} - 1$. Ensinnäkin

$$2^{57885161} = p + 1 \equiv 1 \pmod{p}.$$

Toisaalta, jos α on positiivinen kokonaisluku, joka on pienempi kuin 57885161, niin

$$2 \leqslant 2^{\alpha} < 2^{57885161} = p + 1,$$

ja siten varmasti $2^{\alpha} \not\equiv 1 \pmod{p}$. Siis luvun 2 kertaluku modulo p on 57885161.

On helppo tarkistaa, että $2 \nmid 57885161$ ja $3 \nmid 57885161$. Luentojen lauseen 36 nojalla siis

$$\text{luvun } 4 = 2^2 \text{ kertaluku modulo } p \text{ on } \frac{57885161}{(2, 57885161)} = 57885161,$$

ja

$$\text{luvun } 8 = 2^3 \text{ kertaluku modulo } p \text{ on } \frac{57885161}{(3, 57885161)} = 57885161.$$

2. Määritellään *karakteri* χ modulo 11 seuraavasti: $\chi(2) = -1$, $\chi(0) = 0$, $\chi(m + 11) = \chi(m)$ ja $\chi(mn) = \chi(m)\chi(n)$. Määritä karakterin χ arvo kaikissa jäännösluokissa. (Luku 2 on primitiivinen juuri.)

Ratkaisu. Kolmannen ehdon vuoksi funktion χ arvo $\chi(n)$ riippuu vain luvun n jäännösluokasta modulo 11. Toisen ehdon nojalla $\chi(n) = 0$ kun $11 \mid n$. Ensimmäinen ja neljäs ehto yhdistämällä todetaan, että jokaisella positiivisella kokonaisluvulla α pätee

$$\chi(2^{\alpha}) = \chi(\underbrace{2 \cdot 2 \cdot \ldots \cdot 2}_{\alpha \text{ tekijää}}) = \chi(2)\chi(2)\cdots\chi(2) = (-1)(-1)\cdots(-1) = (-1)^{\alpha}.$$

Koska 2 on primitiivinen juuri modulo 11, käyvät potenssit 2^{α} läpi kaikki nollasta poikkeavat jäännösluokat modulo 11, eli tarvitsee vain laskea kyseiset potenssit (modulo 11):

$$\begin{array}{ll}
-1 = (-1)^1 = \chi(2^1) = \chi(2) & +1 = (-1)^6 = \chi(2^6) = \chi(20) = \chi(9) \\
+1 = (-1)^2 = \chi(2^2) = \chi(4) & -1 = (-1)^7 = \chi(2^7) = \chi(18) = \chi(7) \\
-1 = (-1)^3 = \chi(2^3) = \chi(8) & +1 = (-1)^8 = \chi(2^8) = \chi(14) = \chi(3) \\
+1 = (-1)^4 = \chi(2^4) = \chi(16) = \chi(5) & -1 = (-1)^9 = \chi(2^9) = \chi(6) \\
-1 = (-1)^5 = \chi(2^5) = \chi(10) & +1 = (-1)^{10} = \chi(2^{10}) = \chi(12) = \chi(1)
\end{array}$$

ja kerätä tulokset siistiin taulukkoon:

n	0	1	2	3	4	5	6	7	8	9	10
$\chi(n)$	0	1	-1	1	1	1	-1	-1	-1	1	-1

3. Osoita, että $\sqrt{6}$ on irrationaalinen.

Ratkaisu. Tehdään vastaoletus, ja oletetaan, että $\sqrt{6}$ olisi jokin rationaaliluku $\frac{m}{n}$, missä m ja n ovat kaksi keskenään yhteistekijätöntä positiivista kokonaislukua. Nyt $m^2 = 6n^2$ eli m^2 on parillinen. Siten myös m on parillinen ja $m = 2k$ jollakin positiivisella kokonaisluvulla k. Edelleen $4k^2 = 6n^2$, eli $2k^2 = 3n^2$ ja luvun n^2 on oltava parillinen, eli n on myös parillinen. Mutta nyt luvut m ja n ovat molemmat parillisia, mikä on ristiriidassa sen kanssa ettei niillä ollut yhteisiä tekijöitä.

4. Osoita, että $\sqrt{3} + \sqrt{5}$ on irrationaalinen.

Ratkaisu. Jos luku $\alpha = \sqrt{3} + \sqrt{5}$ olisi rationaalinen, niin olisi myös luku

$$\frac{1}{2}\alpha^2 - 4 = \sqrt{15}$$

rationaalinen, eli riittää osoittaa, että viimeksi mainittu on irrationaalinen. Tämä voidaan tehdä aivan samoin kuin edellisessä tehtävässä.

Oletetaan, että $\sqrt{15}$ olisi jokin rationaaliluku $\frac{m}{n}$, missä m ja n ovat keskenään yhteistekijättömiä positiivisia kokonaislukuja. Nyt $m^2 = 15n^2$, eli $3 \mid m^2$ ja $3 \mid m$, ja voidaan kirjoittaa $m = 3k$ jollakin positiivisella kokonaisluvulla k. Tästä seuraa, että $9k^2 = 15n^2$, ja edelleen, että $3k^2 = 5n^2$. Erityisesti $3 \mid n^2$ ja on oltava $3 \mid n$. Mutta nyt $3 \mid m$ ja $3 \mid n$ vastoin sitä oletusta, ettei luvuilla m ja n ole yhteisiä tekijöitä.

5. Seuraako siitä, että $\alpha > 0$ on irrationaalinen, että $\sqrt[n]{\alpha}$ on irrationaalinen kaikilla positiivisilla kokonaisluvuilla n?

Ratkaisu. Seuraa: jos jokin $\sqrt[n]{\alpha}$ olisi rationaalinen, niin myös

$$\alpha = \underbrace{\sqrt[n]{\alpha}\,\sqrt[n]{\alpha}\cdots\sqrt[n]{\alpha}}_{n \text{ tulontekijää}}$$

olisi rationaalilukujen tulona rationaalinen.

6. Olkoon $n > 1$ kokonaisluku. Osoita, että $\sqrt[n]{n}$ on irrationaalinen.

Ratkaisu. Jos $\sqrt[n]{n}$ olisi jokin rationaaliluku $\frac{a}{b}$, niin olisi oltava $\frac{a^n}{b^n} = n$, mikä on kokonaisluku. Tästä seuraa, että $b^n \mid a^n$, ja esimerkiksi yksikäsitteistä tekijöihinjakoa hyödyntämällä edelleen, että $b \mid a$. Alkuperäinen $\frac{a}{b}$ oli siis kokonaisluku. Eli jos $\sqrt[n]{n}$ on rationaalinen, niin se on kokonaisluku. Koska varmasti $\sqrt[n]{n} > 1$, seuraa ristiriita jos voidaan osoittaa, että $\sqrt[n]{n} < 2$.

Viimeksi mainitun epäyhtälön voi todistaa helposti monilla eri tavoilla. Eräs läpinäkyvä tapa on todistaa induktiolla, että $n < 2^n$. Varmastihan

$$2 < 4 = 2^2.$$

Toisaalta, jos $n < 2^n$, niin

$$n + 1 < 2^n + 1 < 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}.$$