Elementär talteori, våren 2013
Förslag till lösningar för övning 5

1. 25.1.2013 hittades 48. Mersenneprimtalet

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

Vilken ordning har talet 2 i denna modulo? Vilken ordning har talen 4 och 8?

Lösning. Vi beteckar $p = 2^{57885161} - 1$. För det första gäller

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

Å andra sidan, om α är ett positivt heltal mindre än 57885161, så måste

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

och därmed gäller $2^{\alpha} \not\equiv 1 \pmod{p}$. Alltså har talet 2 ordningen 57885161 modulo p.

Vi kan lätt kontrollera att $2 \nmid 57885161$ och $3 \nmid 57885161$. Därmed gäller enligt Sats 36 att

$$\text{talet } 4 = 2^2 \text{ har ordningen } \frac{57885161}{(2, 57885161)} = 57885161 \text{ modulo } p\ ,$$

och att

$$\text{talet } 8 = 2^3 \text{ har ordningen } \frac{57885161}{(3, 57885161)} = 57885161 \text{ modulo } p.$$

2. Låt en *karakter* χ modulo 11 vara följande funktion: $\chi(2) = -1$, $\chi(0) = 0$, $\chi(m + 11) = \chi(m)$ och $\chi(mn) = \chi(m)\chi(n)$. Beräkna karaktärens värde i alla restklasser modulo 11. (Talet 2 är en primitiv rot.)

Lösning. Av det tredje villkoret följer att värdet $\chi(n)$ beror endast på vilken restklass talet n hör till modulo 11. Enligt det andra villkoret gäller $\chi(n) = 0$ då $11 \mid n$. Genom att kombinera villkor 1 och 4 ser vi att det för alla positiva heltal α gäller att

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

Eftersom 2 är en primitiv rot modulo 11, kommer potenserna 2^{α} att gå igenom alla restklasser olika noll modulo 11, så vi måste endast beräkna dessa potenser (modulo 11):

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

Nedan är resultaten samlade i en tabell:

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. Visa, att $\sqrt{6}$ är irrationellt.

Lösning. Vi gör ett motantagande: $\sqrt{6}$ är något rationellt tal $\frac{m}{n}$, var m och n är två positiva heltal som saknar gemensamma delare. Nu gäller $m^2 = 6n^2$, alltså är m^2 jämnt. Därmed är även m ett jämnt tal, alltså gäller $m = 2k$ för något positivt heltal k.

Vidare gäller $4k^2 = 6n^2$, alltså $2k^2 = 3n^2$ och därmed är n^2 ett jämnt tal, alltså är även n jämnt. Men nu är både m och n jämna tal, vilket är en motsägelse eftersom vi antog att de inte har några gemensamma delare.

4. Visa, att $\sqrt{3}+\sqrt{5}$ är irrationellt.

Lösning. Ifall talet $\alpha = \sqrt{3}+\sqrt{5}$ vore rationellt, vore även talet

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

rationellt. Det räcker alltså att visa, att $\sqrt{15}$ är irrationellt. Detta kan vi visa på liknande sätt som vi löste förra uppgiften.

Antag att $\sqrt{15}$ vore något rationellt tal $\frac{m}{n}$, var m och n är två positiva heltal som saknar gemensamma delare. Då gäller $m^2 = 15n^2$, alltså $3 \mid m^2$ och därmed $3 \mid m$, dvs. kan vi skriva $m = 3k$ för något positivt heltal k.

Av detta följer att $9k^2 = 15n^2$, och vidare att $3k^2 = 5n^2$. Alltså gäller $3 \mid n^2$, och därmed följer $3 \mid n$. Men nu gäller $3 \mid m$ och $3 \mid n$ vilket motsäger antagandet att m och n saknar gemensamma delare.

5. Låt talet $\alpha > 0$ vara irrationellt. Gäller det att $\sqrt[n]{\alpha}$ är irrationellt för alla positiva heltal n?

Lösning. Javisst gäller det: ifall $\sqrt[n]{\alpha}$ vore rationellt för något n, vore även

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

rationellt, eftersom det vore en produkt av rationella tal.

6. Låt $n > 1$ vara ett heltal. Visa, att $\sqrt[n]{n}$ är irrationellt.

Lösning. Vi gör igen ett motantagande: Antag att $\sqrt[n]{n}$ är ett rationellt tal $\frac{a}{b}$, var a och b är positiva heltal som saknar gemensamma delare. Av det följer att $\frac{a^n}{b^n} = n$, som är ett heltal, alltså måste $b^n \mid a^n$. Ifall det för något primtal p gäller $p \mid b^n$, måste även $p \mid b$, och eftersom $b^n \mid a^n$, gäller $p \mid a^n$, dvs. $p \mid a$. Eftersom $\operatorname{sgd}(a,b) = 1$, existerar inte något sådant p, alltså måste $b^n = 1$, och därmed följer $b = 1$. Alltså är $\sqrt[n]{n}$ ett heltal a.

Ifall $a = 1$, gäller att $n = (\sqrt[n]{n})^n = 1^n = 1$, vilket är en motsägelse.

Ifall $a > 1$, följer det att $n = a^n \geq 2^n$, vilket är en motsägelse enligt följande induktionsbevis:

Vi vill alltså visa att $n < 2^n$. Klart gäller det att

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

Å andra sidan, om vi antar att $n < 2^n$, så följer

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