Matematiikan koe, Maa11 – Logiikka ja lukuteoria – RATKAISUT **Sievin lukio**
Maanantai 6.5.2013
VASTAA YHTEENSÄ KUUTEEN TEHTÄVÄÄN

---

1. Vastaa lyhyesti, mutta riittävästi.

a) Mitä tarkoitetaan kokonaisluvun alkutekijällä? Jaa luku 40 040 alkutekijöihin.

b) Osoita, että lause $[(p \wedge \neg q) \Longrightarrow r] \Leftrightarrow [\neg r \Longrightarrow (\neg p \vee q)]$ on tautologia. Merkitse pääkonnektiivi näkyviin.

c) Määritä $\text{syt}(54, 153, 171)$ ja $\text{pyj}(54, 153, 171)$. Perustele. Laskin ei riitä perusteluksi.

a) Kokonaisluvun *alkutekijä* on luvun tekijä, joka on alkuluku. Siis, määritteleviä ehtoja on kaksi.

Luvulle 40 040, saadaan

$$40\,040 = 2 \cdot 20\,020 = 2 \cdot 2 \cdot 10\,010 = 2 \cdot 2 \cdot 2 \cdot 5\,005 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 1001$$

$$= 2 \cdot 2 \cdot 2 \cdot 5 \cdot 7 \cdot 143 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 2^3 \cdot 5 \cdot 7 \cdot 11 \cdot 13.$$

b) Laaditaan totuustaulu.

pääkonnektiivi

$[($	p	$\wedge$	$\neg$	q	$)$	$\Longrightarrow$	r	$]$	$\Leftrightarrow$	$[$	$\neg$	r	$\Longrightarrow$	$($	$\neg$	p	$\vee$	q	$)]$
1	0		0	1		1	1		**1**		0	1	1		0	1	1	1	
1	0		0	1		1	0		**1**		1	0	1		0	1	1	1	
1	1		1	0		1	1		**1**		0	1	1		0	1	0	0	
1	1		1	0		0	0		**1**		1	0	0		0	1	0	0	
0	0		0	1		1	1		**1**		0	1	1		1	0	1	1	
0	0		0	1		1	0		**1**		1	0	1		1	0	1	1	
0	0		1	0		1	1		**1**		0	1	1		1	0	1	0	
0	0		1	0		1	0		**1**		1	0	1		1	0	1	0	
1	3		2	1		4	1		**5**		2	1	4		2	1	3	1	

Siis lause $[(p \wedge \neg q) \Longrightarrow r] \Leftrightarrow [\neg r \Longrightarrow (\neg p \vee q)]$ on tautologia.

c) Ratkaistaan ensin syt(54,153), saadaan

$$153 = 54 \cdot 2 + 45, \qquad 54 = 45 \cdot 1 + 9, \qquad 45 = 9 \cdot 5 + 0,$$

eli $\text{syt}(54,153) = 9$. Määritetään sitten syt(9,171), saadaan

$$171 = 9 \cdot 19 + 0,$$

eli $\text{syt}(9,171) = 9$ ja näin ollen $\text{syt}(54,153,171) = 9$.

Ratkaistaan sitten eli pyj(54,153,171). Sitä varten kirjoitetaan luvut alkutekijöiden tulona:

$$54 = 2 \cdot 27 = 2 \cdot 3^3, \qquad 153 = 3 \cdot 51 = 3^2 \cdot 17, \qquad 171 = 3 \cdot 57 = 3^2 \cdot 19.$$

Näin ollen

$$\text{pyj}(54,153,171) = 2 \cdot 3^3 \cdot 17 \cdot 19 = 17\,442.$$

2. a) Miten predikaattilogiikka eroaa propositiologiikasta? **(1)**

b) Selvitä lauseen, i) ja ii) – kohdat, totuusarvo, kun $A = \{0, 1, 2, 3\}$.

i) $\forall x \in A: \exists y \in A: (x - y \in \mathbb{Z})$, **ii)** $\exists x \in A: \forall y \in A: (x - y \in A)$.

Sekä tutki onko lause, iii) ja iv) – kohdat, tosi vai epätosi. Perustele.

iii) $\forall x \in \mathbb{R}_+: \forall y \in \mathbb{R}_+: y < x$, **iv)** $\forall x \in \mathbb{R}_+: \exists y \in \mathbb{R}_+: y < x$. **(5)**

a) Propositiologiikassa tutkitaan suljettuja lauseita, eli niissä lauseissa (= väitteissä) ei ole muuttujaa mukana. Propositiologiikan lauseiden totuusarvo on joko 1 tai 0 (poissulkeva ”joko – tai”, eli ei voi olla molempia), syy *kielletyn ristiriidan laki*. Lisäksi kolmatta vaihtoehtoa ei ole, syy *kielletyn kolmannen vaihtoehdon laki*.

Predikaattilogiikassa tutkitaan avoimia lauseita, joissa on yksi tai useampi muuttuja mukana. Predikaattilogiikan lauseen totuusarvo siis riippuu muuttujan (muuttujien) arvo(i)sta. Propositiologiikassa konnektiivien lisäksi käytössä kvanttorit ∃ ja ∀.

b) Kohdassa **i)** riittää siis löytää kaikille $x \in A$ jokin alkio $y \in A$, jolle erotus $x - y$ on kokonaisluku. Koska erotus on kaikilla x ja y vaihtoehdoilla kokonaisluku, niin lause on aina tosi. Kohdassa **ii)** taas riittää löytää jokin $x \in A$, jolle kaikilla $y \in A$ erotus $x - y$ kuuluu joukkoon A. Jos $x = 0$, niin erotus

vie ulos joukosta A, esimerkiksi $0-1=-1\notin A$. Samoin käy alkioille jos $x=1$ tai $x=2$. Mutta A:n alkiolle $x=3$ erotus $x-y$ pysyy joukossa A kaikilla $y\in A$ ja lause on siis tosi. Saadaan:

x: n arvot	**0**	**0**	**0**	**0**	**1**	**1**	**1**	**1**	**2**	**2**	**2**	**2**	**3**	**3**	**3**	**3**	**nämä ovat lukuja**
y: n arvot	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	
erotus $x-y$	**0**	**−1**	**−2**	**−3**	**1**	**0**	**−1**	**−2**	**2**	**1**	**0**	**−1**	**3**	**2**	**1**	**0**	
i) $x-y\in\mathbb{Z}$	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**nämä ovat totuus-arvoja**
iv) $x-y\in A$	**1**	**0**	**0**	**0**	**1**	**1**	**0**	**0**	**1**	**1**	**1**	**0**	**1**	**1**	**1**	**1**	

Kohdissa **iii)** ja **iv)** joukkona on positiiviset reaaliluvut, eli nolla ei kuulu tähän joukkoon!

Kohta **iii)** ei selvästikään ole totta. Valitaan esimerkiksi $y=5$ ja $x=3$. Tällöin $5\not<3$ ja väite kaatuu. Kohdassa **iv)** pitäisi osoittaa, että kaikille positiivisille reaaliluvuille x löytyy, eli on olemassa, jokin toinen positiivinen reaaliluku y, jolle pätee $y<x$. Tämä väite on totta, sillä luvuksi y voidaan valita luku $\frac{x}{2}$. Nyt $\frac{x}{2}<x$ ja positiivisuus sekä reaalisuus säilyvät, sillä luku x antaa nämä ominaisuudet luvulle $y=\frac{x}{2}$.

Siis **i)** Tosi **ii)** Tosi **iii)** Epätosi **iv)** Tosi.

3. a) Osoita, että kokonaisluku on jaollinen 8:lla, jos ja vain jos sen kolmen viimeisen numeron muodostama luku on jaollinen 8:lla. **(4)**

b) Muunna kymmenjärjestelmään luvut

i) $56,3_8$, ii) $11\,101\,111_2$, ii) FF,A_{16}. **(2)**

a) 8:lla jaollisuus: Olkoon annettuna luku

$$x\equiv a_n10^n+a_{n-1}10^{n-1}+a_{n-2}10^{n-2}+\ \dots\ +a_210^2+a_110^1+a_0.$$

Koska $1000\equiv 8\cdot 125\equiv 0\pmod 8$, niin on $10^i\equiv 0\pmod 8$ kaikilla $i\geq 3$. Näin ollen

$$a_k\cdot 10^k+a_{k-1}\cdot 10^{k-1}+\ \dots\ +a_3\cdot 1000\equiv 0\pmod 8,$$

joten $x\equiv a_2\cdot 100+a_1\cdot 10+a_0\pmod 8$. Siis $8|x$, jos ja vain jos $8|(a_2100+a_110+a_0)$.

b) Muunnetaan luvut kymmenjärjestelmään

i) $56{,}3_8 = 5 \cdot 8^1 + 5 \cdot 8^0 + 5 \cdot 8^{-1} = 40 + 5 + \frac{5}{8} = 45{,}6_{10}$

ii) $11\,101\,111_2 = 1 \cdot 2^7 + 1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$

$$= 128 + 64 + 32 + 0 + 8 + 4 + 2 + 1 = 239_{10}$$

iii) $\mathrm{FF,A}_8 = 15 \cdot 16^1 + 15 \cdot 16^0 + 10 \cdot 16^{-1} = 240 + 15 + \frac{10}{16} = 255{,}625_{10}$

4. a) Ratkaise kongruenssiyhtälö $3x + 15 \equiv 5 \pmod{11}$, mikäli ratkaisu on olemassa.

b) Onko luku $9^9 - 2^9$ jaollinen seitsemällä? Perustele. Laskin ei riitä perusteluksi.

c) Osoita, että jos n on pariton, niin $2n - 1$ on pariton.

a) Muokataan kongruenssiyhtälö $3 \cdot x + 15 \equiv 5 \pmod{11}$ muotoon

$$3 \cdot x \equiv 5 - 15 \equiv -10 \equiv 1 \pmod{11}.$$

Kongruenssiyhtälöstä saadaan Diofantoksen yhtälö

$$3 \cdot x - 11 \cdot y = 1.$$

Luvut 3 ja 11 ovat alkulukuja, joten $\mathrm{syt}(3,11) = 1$ ja ykkönen on itsensä monikerta, eli ratkaisu on olemassa. Kirjoitetaan ykkönen lukujen 3 ja 11 lineaarikombinaationa (ensin Eukleideen algoritmi):

$$11 = 3 \cdot 3 + 2, \qquad 3 = 2 \cdot 1 + 1, \qquad 2 = 1 \cdot 2 + 0\,.$$

$$\Rightarrow \quad 1 = 3 \cdot 1 - 2 \cdot 1 = 3 \cdot 1 - (11 \cdot 1 - 3 \cdot 3) \cdot 1 = 3 \cdot 4 - 11 \cdot 1$$

Siis yksityis- ja yleisratkaisuna Diofantoksen yhtälölle $3 \cdot x - 11 \cdot y = 1$ on

$$\begin{cases} x_0 = 4 \\ y_0 = 1 \end{cases} \quad \Rightarrow \quad \begin{cases} x = 4 + \dfrac{-11}{1}t \\ y = 1 - \dfrac{3}{1}t \end{cases}, \ t \in \mathbb{Z} \quad \Rightarrow \quad \begin{cases} x = 4 - 11t \\ y = 1 - 3t \end{cases}, \ t \in \mathbb{Z}.$$

Ratkaisuksi saadaan siis joukko

$$\{4 - 11t \mid t \in \mathbb{Z}\},$$

joka voidaan myös kirjoittaa muotoon $\{4 + 11\hat{t} \mid \hat{t} \in \mathbb{Z}\}$, koska t on mielivaltainen kokonaisluku.

b) Koska $9 \equiv 2 \pmod{7}$ niin hyödyntämällä tulosta: Jos $a \equiv b \pmod{n}$, niin $a^m \equiv b^m \pmod{n}$ voidaan todeta, että pätee $9^9 \equiv 2^9 \pmod{7}$. Siis $7 | (9^9 - 2^9)$ eli luku $9^9 - 2^9$ on jaollinen 7:llä.

TAI

Hyödynnetään 7:n jaollisuussääntöä:

$$9^9 - 2^9 = 387\,419\,977$$

$$\Rightarrow \quad 387\,419\,97|7 = 387\,419\,97 - 2 \cdot 7 = 38\,741\,983$$

$$\Rightarrow \quad 38\,741\,98|3 = \quad 387\,419\,8 - 2 \cdot 3 \quad = 3\,874\,192$$

$$\Rightarrow \quad 3\,874\,19|2 = \quad 387\,419 - 2 \cdot 2 \quad = 387\,415$$

$$\Rightarrow \quad 387\,41|5 = \quad 38\,741 - 2 \cdot 5 \quad = 38\,731$$

$$\Rightarrow \quad 38\,73|1 = \quad 3\,873 - 2 \cdot 1 \quad = 3\,871$$

$$\Rightarrow \quad 3\,87|1 = \quad 387 - 2 \cdot 1 \quad = 385$$

$$\Rightarrow \quad 38|5 = \quad 38 - 2 \cdot 5 \quad = 28$$

ja tunnetusti $7 \cdot 4 = 28$, eli alkuperäinen luku $9^9 - 2^9 = 387\,419\,977$ on 7:lla jaollinen.

TAI

Luku $9^9 - 2^9$ on jaollinen 7:lla koska $9 - 2 = 7$ ja pätee tulos: $a^n - b^n$ on jaollinen binomilla $a - b$, kun $n \in \mathbb{N}$. Siis

$$9^9 - 2^9 = (9 - 2)(\text{jotain}) = 7 \cdot (\text{jotain}).$$

c) Tämän voi todistaa joko antiteesin avulla tai sitten suoraan. Tehdään molemmilla tavoilla.

Antiteesi: Todistuksen idea on siis tehdä antiteesi, eli vastaoletus:

Oletus: n on pariton, $n \in \mathbb{Z}$.

Väite: $2n - 1$ on pariton.

Todistus: Vastaoletus: $2n - 1$ on parillinen. Tällöin on olemassa $k \in \mathbb{Z}$ siten, että $2n - 1 = 2k$. Tästä seuraa, että

$$2n - 2k = 1 \quad \Rightarrow \quad \underbrace{2(n-k)}_{\text{parillinen}} = \underbrace{1}_{\text{pariton}}.$$

Ristiriita, joten vastaoletus on väärä ja väite oikein.

Suora: Todistuksen idea on käyttää parittoman luvun määritelmää: Luku $n \in \mathbb{Z}$ on pariton, eli on olemassa $k \in \mathbb{Z}$ siten, että $n = 2k + 1$.

Oletus: n on pariton, $n \in \mathbb{Z}$.

Väite: $2n - 1$ on pariton.

Todistus: Määritelmän nojalla $n = 2k + 1$. Tällöin suora lasku antaa

$$2n - 1 \overset{\text{määr.}}{=} 2(2k+1) - 1 = 4k + 2 - 1 = \underbrace{\underbrace{4k}_{\text{parillinen}} + 1}_{\text{pariton}}$$

Siis luku $2n - 1$ on aina pariton, kun n on pariton.

5. Määritellään konnektiivi ”Kaikki tai ei mitään” seuraavasti: $p * q$ tarkoittaa, että joko molemmat (siis p ja q) tai ei kumpikaan (siis ei p eikä q).

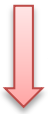
a) Määritä konnektiivi $*$ konnektiiveja $\neg$, $\wedge$ tai $\vee$ käyttäen ja laadi totuustaulu konnektiiville $*$. Merkitse pääkonnektiivi näkyviin.

b) Onko lause $(p * q) \Leftrightarrow (p \Leftrightarrow q)$ tautologia?

a) ”Kaikki tai ei mitään” – konnektiivi $p * q$ tarkoittaa ”p ja q tai ei p ja ei q”, eli

$$p * q \Leftrightarrow [(p \wedge q) \vee (\neg p \wedge \neg q)\,].$$

Laaditaan totuustaulu



pääkonnektiivi

$(p$	$\wedge$	$q)$	$\vee$	$(\neg$	p	$\wedge$	$\neg$	$q)$	$p * q$
1	1	1	**1**	0	1	0	0	1	1
1	0	0	**0**	0	1	0	1	0	0
0	0	1	**0**	1	0	0	0	1	0
0	0	0	**1**	1	0	1	1	0	1
1	3	1	**4**	2	1	3	2	1	5

Totuustaulusta havaitaan, että lause $p * q$ on tosi, jos atomilauseet p ja q ovat molemmat joko tosia tai epätosia. Muulloin lause $p * q$ on epätosi.

b) Taulukkokirjasta tai muistamalla ekvivalenssin totuustaulun todetaan, että konnektiiveilla $*$ ja $\Leftrightarrow$ on täsmälleen samat totuustaulut. Siis lause

$$(p * q) \Leftrightarrow (p \Leftrightarrow q)$$

on tautologia.

6. Osoita MAOL:sta löytyvä tulos

$$\boldsymbol{1^3 + 2^3 + 3^3 + \ \ldots + n^3 = \frac{n^2(n+1)^2}{4}}.$$

(Pelkkä esimerkki jollakin muuttujan n arvolla → 0 pistettä.)

Koska kyseessä on luonnollisia lukuja koskeva tulos, todistetaan se induktiolla.

TOD.: Kun $n = 1$. Tällöin $1^2 = 1 = \frac{4}{4} = \frac{1 \cdot 4}{4} = \frac{1^2 \cdot (1+1)^2}{4}$ ja asia selvä.

Kun $n = k$. Oletetaan, että väite pätee, siis

$$1^3 + 2^3 + 3^3 + \ \ldots + k^3 = \frac{k^2(k+1)^2}{4}.$$

Kun $n = k + 1$. Tällöin

$$\underbrace{1^3 + 2^3 + 3^3 + \ \ldots + k^3}_{= \frac{k^2(k+1)^2}{4},\ \text{ind.ol.nojalla}} + (k+1)^3 = \frac{k^2(k+1)^2}{4} + (k+1)^3$$

$$= \frac{k^2(k+1)^2}{4} + \frac{4(k+1)^2(k+1)}{4}$$

$$= \frac{(k+1)^2[k^2 + 4(k+1)]}{4}$$

$$= \frac{(k+1)^2[k^2 + 4k + 4]}{4}$$

$$= \frac{(k+1)^2(k+2)^2}{4}$$

$$= \frac{(k+1)^2[(k+1)+1]^2}{4}.$$

7. a) Ratkaise yhtälö $[15]_{23}[x]_{23} = [4]_{23}$ lukujoukossa $\mathbb{Z}_{23}$. Miksi ratkaisu on olemassa?

b) Mitkä ovat luvun 99^{1032} kaksi ensimmäistä ja kaksi viimeistä numeroa?

a) Aluksi. Ratkaisu on olemassa, koska 23 on alkuluku. Tuntemattoman ratkaisemiseen voi käyttää joko kokeilua (23 on pieni luku) tai ratkaisemalla Diofantoksen yhtälö $15 \cdot x = 4 \pmod{23}$. Saadaan

Kokeilu:

Kun $x = 1$, niin $[15]_{23}[1]_{23} = [15]_{23} \neq [4]_{23}$.

Kun $x = 2$, niin $[15]_{23}[2]_{23} = [30]_{23} = [7]_{23} \neq [4]_{23}$.

Kun $x = 3$, niin $[15]_{23}[3]_{23} = [45]_{23} = [22]_{23} \neq [4]_{23}$.

Kun $x = 4$, niin $[15]_{23}[4]_{23} = [60]_{23} = [14]_{23} \neq [4]_{23}$.

Kun $x = 5$, niin $[15]_{23}[5]_{23} = [75]_{23} = [6]_{23} \neq [4]_{23}$.

Kun $x = 6$, niin $[15]_{23}[6]_{23} = [90]_{23} = [21]_{23} \neq [4]_{23}$.

Kun $x = 7$, niin $[15]_{23}[7]_{23} = [105]_{23} = [13]_{23} \neq [4]_{23}$.

Kun $x = 8$, niin $[15]_{23}[8]_{23} = [120]_{23} = [5]_{23} \neq [4]_{23}$.

Kun $x = 9$, niin $[15]_{23}[9]_{23} = [135]_{23} = [20]_{23} \neq [4]_{23}$.

Kun $x = 10$, niin $[15]_{23}[10]_{23} = [150]_{23} = [12]_{23} \neq [4]_{23}$.

Kun $x = 11$, niin $[15]_{23}[11]_{23} = [165]_{23} = [4]_{23}$.

Siis $[x]_{23} = [11]_{23}$.

TAI

Ratkaistaan kongruenssiyhtälö $15 \cdot x \equiv 4 \pmod{23}$. Saadaan Diofantoksen yhtälö

$$15 \cdot x - 23 \cdot y = 4.$$

Tai sama yhtälö toisin kirjoitettuna $15 \cdot x - 4 = 23 \cdot y$. Joka tapauksessa koska $\text{syt}(15,23) = 1$ (luku 23 on siis alkuluku) ja neljä on ykkösen monikerta, niin ratkaisu on olemassa. Kirjoitetaan ykkönen lukujen 15 ja 23 lineaarikombinaationa (ensin Eukleideen algoritmi):

$$23 = 15 \cdot 1 + 8, \qquad 15 = 8 \cdot 1 + 7, \qquad 8 = 7 \cdot 1 + 1, \qquad 7 = 1 \cdot 7 + 0\,.$$

$$\Rightarrow \quad 1 = 8 \cdot 1 - 7 \cdot 1 = 8 \cdot 1 - (15 \cdot 1 - 8 \cdot 1) \cdot 1$$

$$= (23 \cdot 1 - 15 \cdot 1) \cdot 1 - (15 \cdot 1 - (23 \cdot 1 - 15 \cdot 1) \cdot 1) \cdot 1$$

$$= 23 \cdot 2 - 15 \cdot 3$$

Merkitään vielä kertoimien etumerkit samoin, kuin oli alkuperäisessä yhtälössä $15 \cdot x - 23 \cdot y = 4$. Siis $1 = -23 \cdot (-2) + 15 \cdot (-3)$. Nyt luku 4 voidaan kirjoittaa lineaarikombinaationa

$$4 = 15 \cdot (-12) - 23 \cdot (-8).$$

Siis yksityis- ja yleisratkaisuna Diofantoksen yhtälölle $15 \cdot x - 23 \cdot y = 4$ on

$$\begin{cases} x_0 = -12 \\ y_0 = -8 \end{cases} \quad \Rightarrow \quad \begin{cases} x = -12 + \dfrac{-23}{1}t \\ y = -8 - \dfrac{15}{1}t \end{cases}, \ t \in \mathbb{Z} \quad \Rightarrow \quad \begin{cases} x = -12 - 23t \\ y = -8 - 15t \end{cases}, \ t \in \mathbb{Z}.$$

Ratkaisuna alkuperäiseen kysymykseen on x, eli joukko

$$\{-12 - 23t \mid t \in \mathbb{Z}\} = \{11 - 23\hat{t} \mid \hat{t} \in \mathbb{Z}\},$$

ja tapana on valita alkio, joka kuuluu välille $0 - 22$, siis tässä tapauksessa 11.

b) Kaksi viimeistä numeroa:

Aluksi havaitaan, koska tarkastellaan kahta viimeistä numeroa, että

$$99 \equiv -1 \pmod{100}.$$

Näin ollen

$$99^{1032} \equiv (-1)^{1032} \equiv 1 \pmod{100}.$$

Siis luvun 99^{1032} kaksi viimeistä numeroa ovat **0** ja **1**.

Kaksi ensimmäistä numeroa:

Kirjoitetaan potenssi sellaiseen muotoon, että sulkujen sisällä on luku, jonka laskin antaa kymmen-potenssimuodossa ja edetään siitä eteenpäin. Esimerkiksi näin

$$99^{1032} = 99^{50 \cdot 20 + 32} = (99^{50})^{20} \cdot 99^{32} = (6{,}0500606 \ldots \cdot 10^{99})^{20} \cdot 7{,}2498033 \ldots \cdot 10^{63}$$

$$= 6{,}0500606 \ldots^{20} \cdot 10^{1980} \cdot 7{,}2498033 \ldots \cdot 10^{63}$$

$$= \underbrace{6{,}0500606 \ldots^{20} \cdot 7{,}2498033 \ldots}_{= 3{,}1298305 \ldots \cdot 10^{16}} \cdot \underbrace{10^{63} \cdot 10^{1980}}_{= 10^{2043}}$$

$$= 3{,}1298305 \ldots \cdot 10^{16+2043} = 3{,}12 \ldots \cdot 10^{2059}$$

Siis luvun 99^{1032} kaksi ensimmäistä numeroa ovat **3** ja **1**.

TAI

Käyttää logaritmeja.

8. a) Ratkaise kongruenssiyhtälö $x^2 \equiv 2 \pmod{17}$,

b) Onko $12^{522} \equiv 35 \pmod{53}$. Perustele.

a) Taulukoidaan arvot, kun $x \in \{0,1,2,\ldots,17\}$, saadaan

x	0	1	2	3	4	5	**6**	7	8	9	10	**11**	12	13	14	15	16	17
x^2	0	1	4	9	16	25	**36**	49	64	81	100	**121**	144	169	196	225	256	298
mod 17	0	1	4	9	16	8	**2**	15	13	13	15	**2**	8	16	9	4	1	0

Vastaus:

$$\begin{cases} x = 6 + 17t \\ x = 11 + 17t' \end{cases} \qquad t \in \mathbb{Z}$$

b) Kongruenssien laskusääntöjä sekä Fermat'n pientä lausetta käyttämällä, saadaan

$$12^{522} \equiv 12^{52 \cdot 10 + 2} \equiv (12^{52})^{10} \cdot 12^2 \overset{\text{Fermat}}{\equiv} 1^{10} \cdot 144 \equiv 53 \cdot 2 + 38 \equiv 38 \pmod{53},$$

eli ei ole.

9. JOKERI* (9p)

a) Olkoon n alkuluku sekä x ja y kokonaislukuja. Osoita, että

$$x^n + y^n \equiv (x + y)^n \pmod{n}.$$

YO – K2007/13.

b) Etsi jakojäännös, kun i) 2^{345} jaetaan luvulla 5, ii) 3^{4567} jaetaan luvulla 6.

YO – S2005/15.

a) Fermat'n pienen lauseen mukaan $a^{n-1} \equiv 1 \pmod{n}$, missä n on alkuluku, joka ei ole kokonaisluvun a tekijä, eli $n \nmid a$ tai $\text{syt}(a, n) = 1$. Tällöin pätee $a^n \equiv a \pmod{n}$. Kongruenssin molemmat puolet on siis kerrottu a:lla.

Toisaalta, jos n on luvun a tekijä, on n myös luvun a^n tekijä. Tällöin

$$a \equiv 0 \pmod{n} \qquad \text{ja} \qquad a^n \equiv 0 \pmod{n}.$$

Siis, jokaisella alkuluvulla n pätee $a^n \equiv a \pmod{n}$.

Koska x ja y ovat kokonaislukuja, on

$$x^n \equiv x \pmod{n} \qquad \text{ja} \qquad y^n \equiv y \pmod{n},$$

joten kongruenssien laskusääntöjä käyttäen molemmat puolet voidaan summata keskenään, saadaan

$$x^n + y^n \equiv x + y \pmod{n}.$$

Summa $x + y$ on jokin kokonaisluku, joten

$$(x + y)^n \equiv x + y \pmod{n}.$$

Yhdistämällä kaksi edellistä tulosta saadaan väite, siis

$$(\boldsymbol{x + y})^{\boldsymbol{n}} \equiv x + y \equiv \boldsymbol{x^n + y^n} \pmod{\boldsymbol{n}}.$$

b) Tarkastellaan lukua $2^{345} \pmod{5}$:ssä. Koska $4 \equiv -1 \pmod{5}$, niin saadaan

$$2^{345} \equiv 2 \cdot 2^{344} \equiv 2 \cdot 2^{2 \cdot 172} \equiv 2 \cdot (2^2)^{172} \equiv 2 \cdot (4)^{172} \equiv 2 \cdot (-1)^{172} \equiv 2 \cdot 1 \equiv 2 \pmod{5}.$$

Siis, jakojäännös on 2.

Luvun 3^{4567} tapauksessa merkitään jakojäännöstä r:llä, jolloin pätee $0 \leq r < 6$. Nyt on siis olemassa luku $n \in \mathbb{Z}$ siten, että

$$3^{4567} = 6n + r.$$

Tästä muokkaamalla saadaan

$$3 \cdot 3^{4566} = 6n + r \quad \overset{\text{jaetaan } 3\text{:}lla}{\Rightarrow} \quad 3^{4566} = 2n + \frac{r}{3}.$$

Toisaalta luku 3^{4566} on pariton (parittoman luvun 3 potenssina…tämä pitäisi tietysti todistaa…induktiolla) ja koska $0 \leq r < 6$, niin milloin luku $2n + \frac{r}{3}$ on pariton? Silloin, kun $r = 3$.

Siis, jakojäännös on 3.

TAI

Tarkastellaan potenssien $2^n, n = 1,2,3, \ldots$ jakojäännöksiä jaettaessa luvulla 5 ja huomataan (todistus induktio), että ne toistuvat neljän luvun $2, 4, 3$ ja 1 jaksoissa. Siis

$$2^1 \equiv 2 \pmod{5}, \qquad 2^2 \equiv 4 \pmod{5}, \qquad 2^3 \equiv 8 \equiv 3 \pmod{5}, \qquad 2^4 \equiv 16 \equiv 1 \pmod{5},$$

$2^5 \equiv 32 \equiv 2 \pmod 5$, $2^6 \equiv 64 \equiv 4 \pmod 5$, $2^7 \equiv 128 \equiv 3 \pmod 5$, jne.

Koska $345 = 86 \cdot 4 + 1$, niin potenssin 2^{345} jakojäännös on jakson ensimmäinen eli 2.

Vastaavalla tavalla havaitaan (todistus induktio), että potenssin $3^n, n = 1,2,3, \ldots$ jakojäännös luvulla 6 jaettaessa on aina 3. Siis

$3^1 \equiv 3 \pmod 6$, $3^2 \equiv 9 \equiv 3 \pmod 6$, $3^3 \equiv 27 \equiv 3 \pmod 6$,

$3^4 \equiv 81 \equiv 3 \pmod 6$, $3^5 \equiv 243 \equiv 3 \pmod 6$, $3^6 \equiv 729 \equiv 3 \pmod 6$, jne.