19. Astmetsüklid

Olgu antud positiivsed täisarvud a ja n ning vaatleme a järjestikuste astmete jääke jagamisel n-ga:

$$a^0 \bmod n, \quad a^1 \bmod n, \quad a^2 \bmod n, \quad a^3 \bmod n, \ldots .$$

Teame, et n-ga jagamisel saab jääkidena tekkida ainult n erinevat arvu $(0, 1, \ldots, n-1)$. Teisest küljest on astmete jääkide jada iga järgmine liige eelmise poolt üheselt määratud, sest

$$a^{i+1} \bmod n = a \cdot (a^i \bmod n) \bmod n. \tag{19.1}$$

Järelikult peab vaadeldavas jadas tekkima tsükkel. See tähelepanek on kasulik suurte astmete jääkide leidmisel.

▪ **Näide 19.1** Mis on $2^{2023} \bmod 30$? Leiame arvu 2 esimeste astmete jäägid modulo 30:

$$\begin{aligned}
2^0 &= 1 \equiv 1 \bmod 30,\\
2^1 &= 2 \equiv 2 \bmod 30,\\
2^2 &= 4 \equiv 4 \bmod 30,\\
2^3 &= 8 \equiv 8 \bmod 30,\\
2^4 &= 16 \equiv 16 \bmod 30,\\
2^5 &= 32 \equiv 2 \bmod 30,\\
2^6 &= 64 \equiv 4 \bmod 30,\\
2^7 &= 128 \equiv 8 \bmod 30,\\
2^8 &= 256 \equiv 16 \bmod 30.
\end{aligned}$$

Näeme, et tekib tsükkel $2, 4, 8, 16$ pikkusega 4. Kuna $2023 \equiv 3 \bmod 4$, siis

$$2^{2023} \equiv 2^3 = 8 \bmod 30.$$

▪

Paneme tähele, et seos (19.1) võimaldab meil arvutuste käigus arvude liiga suureks minekut vältida, sest igal sammul saame väärtusi asendada nende jääkidega mooduli n järgi. Näiteks

$$2^6 \equiv 2 \cdot (2^5 \bmod 30) \equiv 2 \cdot 2 = 4 \bmod 30.$$

Ülesanded

Ülesanne 19.1 (Lõppvoor 1993, 9. klass) Tõesta, et arv $7^{1993} + 1993$ jagub arvuga 100.

Ülesanne 19.2 (Lõppvoor 1998, 9. klass) Leia arvu 11^{1998} kaks viimast numbrit.

Ülesanne 19.3 (Piirkonnavoor 1993, 10. klass) Tõesta, et $101^{100} - 1$ jagub arvuga 24.

Ülesanne 19.4 (Lõppvoor 1998, 10. klass) Tõesta, et kui positiivse täisarvu n korral on $5^n + 3^n + 1$ algarv, siis n jagub arvuga 12.

Ülesanne 19.5 (Piirkonnavoor 1994, 12. klass) Leia kõik naturaalarvud n, mille korral arv $1^n + 2^n + 3^n + 4^n$ jagub arvuga 5.

Ülesanne 19.6 (Lõppvoor 1996, 11. klass) Tõesta, et arv $1^n + 2^n + \ldots + 15^n$ jagub arvuga 480 mistahes paaritu arvu $n \geqslant 3$ korral.

Ülesanne 19.7 (Lõppvoor 2021, 11. klass) Tõesta, et arv $2021^{2020} + 5$ jagub arvuga 63.

Ülesanne 19.8 (Lõppvoor 1999, 12. klass) Olgu a, b, c ja d mittenegatiivsed täisarvud. Tõesta, et arvud $2^a 7^b$ ja $2^c 7^d$ annavad 15-ga jagamisel sama jäägi siis ja ainult siis, kui arvud $3^a 5^b$ ja $3^c 5^d$ annavad 16-ga jagamisel sama jäägi.

Ülesanne 19.9 (Lõppvoor 1996, 12. klass) Tõesta, et mistahes algarvu $p > 5$ korral leidub selline positiivne täisarv n, et arvu p^n kümnendesituse kolm viimast numbrit on 001.

Ülesanne 19.10 (Lõppvoor 2001, 12. klass) Tõesta, et iga täisarvu $a > 1$ jaoks leidub niisugune algarv p, et

$$1 + a + a^2 + \ldots + a^{p-1}$$

on kordarv.

Ülesanne 19.11 (Lõppvoor 2011, 12. klass) Leia arvu

$$1^1 + 2^2 + 3^3 + \ldots + 2011^{2011}$$

viimane number.

Lahendused

19.1 Uurides arvu 7 astmeid leiame, et

$$7^0 = 1, \quad 7^1 = 7, \quad 7^2 = 49, \quad 7^3 = 343, \quad 7^4 = 2401,$$

niisiis

$$7^0 \equiv 7^4 \equiv 1 \bmod 100.$$

See tähendab, et 7 astmed modulo 100 annavad tsükli pikkusega 4 ja $7^i \equiv 1 \bmod 100$ alati, kui $i \vdots 4$. Muuhulgas $7^{1992} \equiv 1 \bmod 100$ ja järelikult $7^{1993} \equiv 7 \bmod 100$, mistõttu

$$7^{1993} + 1993 \equiv 7 + 93 \equiv 0 \bmod 100\,,$$

mida oligi tarvis tõestada.

19.2 Vastus: 81.

Uurime arvu 11 astmete jääkide tsüklit mooduli 100 järgi. Arvutades peame meeles, et iga tehte järel võime leitud väärtuse asendadad tema jäägiga modulo 100. Nii väldime arvutuste käigus arvude liiga suureks minemist.

$$\begin{aligned}
11^0 &\equiv 1 \bmod 100\,,\\
11^1 &\equiv 11 \bmod 100\,,\\
11^2 = 121 &\equiv 21 \bmod 100\,,\\
11^3 \equiv 11 \cdot 21 = 231 &\equiv 31 \bmod 100\,,\\
11^4 \equiv 11 \cdot 31 = 341 &\equiv 41 \bmod 100\,,\\
&\dots\\
11^9 \equiv 11 \cdot 81 = 891 &\equiv 91 \bmod 100\,,\\
11^{10} \equiv 11 \cdot 91 = 1001 &\equiv 1 \bmod 100\,,\\
11^{11} \equiv 11 \cdot 1 = 11 &\equiv 11 \bmod 100\,,\\
&\dots
\end{aligned}$$

Näeme, et tekib tsükkel pikkusega 10, kusjuures $11^n \equiv 1 \bmod 100$ parajasti siis, kui $n \,\vdots\, 10$. Järelikult

$$11^{1998} \equiv 11^8 \equiv 81 \bmod 100\,.$$

19.3 Piisab kui tõestame, et $101^{100} - 1$ jagub nii 3-ga kui 8-ga.

Kuna $101 \equiv 2 \bmod 3$ võime uurida arvu 2 astmete käitumist modulo 3. Näeme, et

$$2^0 \equiv 1 \bmod 3, \quad 2^1 \equiv 2 \bmod 3, \quad 2^2 = 4 \equiv 1 \bmod 3, \quad 2^3 = 8 \equiv 2 \bmod 3, \dots\,.$$

Saame tsükli pikkusega 2, kusjuures paarisarvuliste astmete puhul tekib jääk 1. Niisiis

$$101^{100} - 1 \equiv 2^{100} - 1 \equiv 1 - 1 = 0 \bmod 3\,.$$

Mooduli 8 järgi saame $101 \equiv 5 \bmod 8$, seega võime uurida arvu 5 astmeid modulo 8:

$$5^0 \equiv 1 \bmod 8,\ 5^1 \equiv 5 \bmod 8,\ 5^2 = 25 \equiv 1 \bmod 8,\ 5^3 = 125 \equiv 5 \bmod 8, \dots\,.$$

Saame tsükli pikkusega 2, kusjuures paarisarvuliste astmete puhul tekib jääk 1. Niisiis

$$101^{100} - 1 \equiv 5^{100} - 1 \equiv 1 - 1 = 0 \bmod 8\,.$$

Muidugi võime mooduli 8 jaoks kasutada ka tähelepanekut, et iga paaritu arvu ruut annab 8-ga jagades jäägi 1. Tõepoolest, $(2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$. Kuna k ja $k+1$ on kaks järjestikust täisarvu, peab üks neist kindlasti 2-ga jaguma, mistõttu $4k(k+1)$ jagub 8-ga. Kuna $101^{100} = (101^{50})^2$ ja 101^{50} on paaritu arv, peab kehtima kongruents $101^{100} \equiv 1 \bmod 8$.

Selle ülesande veel ühe võimaliku lahenduse annab ülesanne kui 24.2.

19.4 Näitame, et alati, kui n annab 12-ga jagades jäägi, mis erineb 0-st, peab ülesande avaldise väärtus olema kordarvuline.

Uurime kõigepealt arvu 5 astmete tsüklit modulo 3:

$$5^0 \equiv 1 \bmod 3, \quad 5^1 \equiv 2 \bmod 3, \quad 5^2 = 25 \equiv 1 \bmod 3, \quad 5^3 = 125 \equiv 2 \bmod 3.$$

Näeme, et tekib tsükkel pikkusega 2, kusjuures $5^n \equiv 2 \bmod 3$ parajasti siis, kui n on paaritu. See tähendab, et paaritu n korral

$$5^n + 3^n + 1 \equiv 2 + 0 + 1 \equiv 0 \bmod 3.$$

Kuna $5^n + 3^n + 1 > 3$, peab tegemist olema 3-ga jaguva kordarvuga.

Teiseks uurime arvu 3 astmete tsüklit modulo 5.

$$\begin{aligned} 3^0 &\equiv 1 \bmod 5, \\ 3^1 &\equiv 3 \bmod 5, \\ 3^2 = 9 &\equiv 4 \bmod 5, \\ 3^3 = 27 &\equiv 2 \bmod 5, \\ 3^4 = 81 &\equiv 1 \bmod 5. \end{aligned}$$

Niisiis tekib tsükkel pikkusega 4, kusjuures $3^n \equiv 4 \bmod 5$ parajasti siis, kui $n \equiv 2 \bmod 4$. See tähendab, et kui n annab 12-ga jagades jäägi $2, 6$ või 10, siis

$$5^n + 3^n + 1 \equiv 0 + 4 + 1 \equiv 0 \bmod 5.$$

Kuna $5^n + 3^n + 1 > 5$, peab tegemist olema 5-ga jaguva kordarvuga.

Viimaks uurime kogu ülesande avaldise jääki modulo 7. Koostame tabeli, kuhu kirjutame arvude 5^n, 3^n ja 1 ning nende summa jäägi jagamisel 7-ga.

n	0	1	2	3	4	5	6
$5^n \bmod 7$	1	5	4	6	2	3	1
$3^n \bmod 7$	1	3	2	6	4	5	1
$1 \bmod 7$	1	1	1	1	1	1	1
$\sum \bmod 7$	3	2	0	6	0	2	3

Tekib tsükkel pikkusega 6, kusjuures $5^n + 3^n + 1 \vdots 7$ parajasti siis, kui n annab 6-ga jagades jäägi 2 või 4. Kuna $5^n + 3^n + 1 > 7$ tähendab see, et ülesande avaldis annab 7-ga jaguva kordarvu, kui n-i jääk jagamisel 12-ga on $2, 4, 8$ või 10.

Kokkuvõttes oleme näidanud, et $5^n + 3^n + 1$ on kordarv alati, kui n annab 12-ga jagades mingi muu jäägi kui 0. Seega kui $5^n + 3^n + 1$ on algarv, peab n jaguma 12-ga.

On võimalik näidata, et $5^n + 3^n + 1$ on algarv näiteks siis, kui $n = 12, 36, 48, 72$ või 120.

19.5 Vastus: sobivad parajasti kõik n väärtused, kus n ei jagu 4-ga.

Vaatleme a^n jääke jagamisel 5-ga, kus $a = 1, 2, 3, 4$ ja $n = 0, 1, 2, 3, 4$. Koostame tabeli, mille viimasele reale arvutame veeruelementide summa jäägi jagamisel 5-ga.

n	0	1	2	3	4
$1^n \bmod 5$	1	1	1	1	1
$2^n \bmod 5$	1	2	4	3	1
$3^n \bmod 5$	1	3	4	2	1
$4^n \bmod 5$	1	4	1	4	1
$\sum \bmod 5$	4	0	0	0	4

Näeme, et arvu 1 astmed moodustavad tsükli pikkusega 1, arvude 2 ja 3 astmed tsükli pikkusega 4 ning arvu 4 astmed tsükli pikkusega 2. Kogu tabel hakkab seega korduma tsüklis pikkusega 4. Seega hakkab samas tsüklis korduma ka veeruelementide summa jääk jagamisel 5-ga. Tabelist näeme, et veerud, kus summa jääk ei tule 0, on parajasti need, kus $n \vdots 4$.

19.6 Kuna $480 = 2^5 \cdot 3 \cdot 5$, uurime ülesande avaldist eraldi moodulite 3, 5 ja 32 järgi.

Kõigepelt koostame tabeli, kuhu leiame a^n jäägid ja nende jääkide summa jagamisel 3-ga, kus $a = 1, 2, 3$.

n	1	2	3	4
$1^n \bmod 3$	1	1	1	1
$2^n \bmod 3$	2	1	2	1
$3^n \bmod 3$	0	0	0	0
$\sum \bmod 3$	0	2	0	2

Näeme, et 1^n ja 3^n annavad tsükli pikkusega 1, 2^n aga tsükli pikkusega 2. Nende summa annab järelikult samuti tsükli pikkusega 2, kusjuures paarituarvuliste n väärtuste puhul jagub summa 3-ga.

Kuna $1 \equiv 4 \equiv 7 \equiv \ldots \equiv 13 \bmod 3$, $2 \equiv 5 \equiv 8 \equiv \ldots \equiv 14 \bmod 3$ ja $3 \equiv 6 \equiv 9 \equiv \ldots \equiv 15 \bmod 3$, kehtib täpselt sama arutelu ka kolmikute $(4,5,6), (7,8,9), \ldots, (13,14,15)$ jaoks. Kokkuvõttes saame, et ülesande avaldis jagub 3-ga iga paaritu astendaja n korral.

Mooduli 5 järgi saame arutleda sarnaselt, uurides kõigepealt summat $1^n + 2^n + 3^n + 4^n + 5^n$. Vastav arutelu kordab sisuliselt ülesande 19.5 lahendust ainult selle erinevusega, et nüüd liidame ka väärtuse 5^n, mis ei muuda aga midagi, sest $5^n \equiv 0 \bmod 5$. Ülesande 19.5 lahendusest järeldub, et

$$1^n + 2^n + 3^n + 4^n + 5^n \equiv 0$$

iga paarituarvulise n väärtuse korral. Jääb veel ainult tähele panna, et

$$1^n + 2^n + 3^n + 4^n + 5^n \equiv 6^n + 7^n + 8^n + 9^n + 10^n \equiv 11^n + 12^n + 13^n + 14^n + 15^n \bmod 5\,,$$

mistõttu ka

$$1^n + 2^n + \ldots + 15^n \equiv 0 \bmod 5\,.$$

Mooduli 32 järgi uurime kõigepealt summat $1^n + 15^n$. Kuna n on paaritu, saame selle summa tegurdada (vt harjutus 10.4 peatükist 10):

$$1^n + 15^n = (1+15)(1^{n-1} - 1^{n-2} \cdot 15 + 1^{n-3} \cdot 15^2 - \ldots + 1^2 \cdot 15^{n-3} - 1 \cdot 15^{n-2} + 15^{n-1})\,.$$

Esimese teguri väärtus on $1 + 15 = 16$, teine tegur aga on paaritu, sest temas on n paarituarvulist liidetavat-lahutatavat.

Täpselt sama moodi leiame, et arvud $3^n + 13^n$, $5^n + 11^n$ ja $7^n + 9^n$ on arvu 16 ja mingi paaritu arvu korrutised. Järelikult

$$1^n + 3^n + 5^n + 7^n + 9^n + 11^n + 13^n + 15^n \vdots 32\,.$$

Teisest küljest

$$2^n + 14^n = (2+14)(2^{n-1} - 2^{n-2}\cdot 14 + 2^{n-3}\cdot 14^2 - \ldots + 2^2\cdot 14^{n-3} - 2\cdot 14^{n-2} + 14^{n-1})$$

on 16 ja mingi paarisarvu korrutis ning jagub seetõttu 32-ga; sama arutelu kehtib muidugi ka summade $4^n + 12^n$ ja $6^n + 10^n$ kohta.

Lõpetuseks jääb veel tähele panna, et 8^n jagub 32-ga alati, kui $n \geqslant 2$.

Kokkuvõttes oleme tõestanud, et ülesande avaldis jagub arvuga 480 iga paaritu arvu $n \geqslant 3$ korral.

Ülesande algses sõnastuses küsiti tõestust ainult $n \geqslant 5$ jaoks.

19.7 Uurime ülesande avaldist eraldi moodulite 7 ja 9 järgi.

Paneme tähele, et $2021 - 5 = 2016$ ning et $2016 \vdots 7$ ja $2016 \vdots 9$. Järelikult $2021 \equiv 5 \bmod 7$ ja $2021 \equiv 5 \bmod 9$ ning meil piisab tõestada, et arv $5^{2020} + 5$ jagub 7-ga ja 9-ga.

Uurime arvu 5 astmete tsüklit modulo 7.

$$\begin{aligned}
5^0 &\equiv 1 \bmod 7\,,\\
5^1 &\equiv 5 \bmod 7\,,\\
5^2 = 25 &\equiv 4 \bmod 7\,,\\
5^3 \equiv 5\cdot 4 = 20 &\equiv 6 \bmod 7\,,\\
5^4 \equiv 5\cdot 6 = 30 &\equiv 2 \bmod 7\,,\\
5^5 \equiv 5\cdot 2 = 10 &\equiv 3 \bmod 7\,,\\
5^6 \equiv 5\cdot 3 = 15 &\equiv 1 \bmod 7\,.
\end{aligned}$$

Näeme, et tekib tsükkel pikkusega 6. Kuna $2020 \equiv 4 \bmod 6$, saame

$$2021^{2020} + 5 \equiv 5^{2020} + 5 \equiv 5^4 + 5 \equiv 2 + 5 \equiv 0 \bmod 7\,,$$

järelikult jagub arv $2021^{2020} + 5$ arvuga 7.

Uurime arvu 5 astmete tsüklit modulo 9.

$$\begin{aligned}
5^0 &\equiv 1 \bmod 9\,,\\
5^1 &\equiv 5 \bmod 9\,,\\
5^2 = 25 &\equiv 7 \bmod 9\,,\\
5^3 \equiv 5\cdot 7 = 35 &\equiv 8 \bmod 9\,,\\
5^4 \equiv 5\cdot 8 = 40 &\equiv 4 \bmod 9\,,\\
5^5 \equiv 5\cdot 4 = 20 &\equiv 2 \bmod 9\,,\\
5^6 \equiv 5\cdot 2 = 10 &\equiv 1 \bmod 9\,.
\end{aligned}$$

Näeme, et jälle tekib tsükkel pikkusega 6. Eelmise juhuga analoogiliselt saame

$$2021^{2020} + 5 \equiv 5^{2020} + 5 \equiv 5^4 + 5 \equiv 4 + 5 \equiv 0 \bmod 9\,,$$

järelikult jagub arv $2021^{2020}+5$ ka arvuga 9 ning kokkuvõttes arvuga 63.

Julgemad lahendajad[1] võivad kohe uurida arvu 5 astmete tsüklit modulo 63.

$$\begin{aligned}
5^0 &\equiv 1 \bmod 63\,,\\
5^1 &\equiv 5 \bmod 63\,,\\
5^2 &\equiv 25 \bmod 63\,,\\
5^3 = 125 &\equiv 62 \bmod 63\,,\\
5^4 = 625 &\equiv 58 \bmod 63\,,\\
5^5 \equiv 5\cdot 58 \equiv 5\cdot(-5) = -25 &\equiv 38 \bmod 63\,,\\
5^6 \equiv 5\cdot 38 = 190 &\equiv 1 \bmod 63\,.
\end{aligned}$$

Näeme, et tekib tsükkel pikkusega 6. Kuna $2020 \equiv 4 \bmod 6$, saame

$$2021^{2020}+5 \equiv 5^{2020}+5 \equiv 5^4+5 \equiv 58+5 \equiv 0 \bmod 63\,,$$

järelikult jagub arv $2021^{2020}+5$ arvuga 63.

Veel ühe võimaliku lahenduse annab ülesanne 24.5

19.8 Uurime astmete 2^n, 7^n jääkide tsükleid modulo 15 ning 3^n ja 5^n jääkide tsükleid modulo 16. Koostame tabeli:

n	0	1	2	3	4
$2^n \bmod 15$	1	2	4	8	1
$7^n \bmod 15$	1	7	4	13	1
$3^n \bmod 16$	1	3	9	11	1
$5^n \bmod 16$	1	5	9	13	1

Näeme, et alati tekib tsükkel pikkusega 4. Niisiis võime ülesandes esinevad astendajad alati asendada nende jääkidega modulo 4, mistõttu piisab vaadelda juhtu, kui $a, b, c, d \in \{0,1,2,3\}$.

Koostame nüüd kaks eraldi tabelit, milles leiame $2^m 7^n \bmod 15$ ja $3^m 5^n \bmod 16$ kõikvõimalikud väärtused, kui $m, n \in \{0,1,2,3\}$.

7^n \ 2^m	1	2	4	8
1	1	2	4	8
7	7	14	13	11
4	4	8	1	2
13	13	11	7	14

5^n \ 3^m	1	3	9	11
1	1	3	9	11
5	5	15	13	7
9	9	11	1	3
13	13	7	5	15

Nüüd saame vahetult kontrollida, et $2^a7^b \equiv 2^c7^d$ ja $3^a5^b \equiv 3^c5^d$ parajasti siis, kui:

- $a = c$ ja $b = d$; või
- $|a-c| = 2$ ja $|b-d| = 2$.

Mõlemas tabelis on samad jäägid jälgitavuse huvides ka sama värviga märgistatud.

[1]Julgust läheb vaja sellepärast, et tekkiv tsükkel võib osutuda pikaks. Otsides tsükleid eraldi modulo 7 ja 9 garanteerime, et need ei saa olla pikemad kui vastavalt 7 ja 9 elementi.

19.9 Peame näitama, et leidub $n \geqslant 1$ nii, et $p^n \equiv 1 \bmod 1000$. Paneme tähele, et $p^0 \equiv 1 \bmod 1000$. Kui meil õnnestub tõestada, et $p^n \bmod 1000$ jõuab tsükliga tagasi 1-ni, on ülesanne lahendatud.

Me teame juba, et p astmetes mooduli 1000 järgi peab tsükkel kindlasti tekkima, aga kas see tsükkel peab alati alagama jada esimesest elemendist? Näide 19.1 tõestab, et mitte tingimata: $2^0 \equiv 1 \bmod 30$, aga tsükkel algab alles väärtusest $2^1 = 2$.

Mille poolest näide 19.1 ja praegune ülesanne erinevad? Paneme tähele, et ülesandes 19.1 polnud astendatav 2 ja moodul 30 ühistegurita, siinses ülesandes aga $\text{SÜT}(p, 1000) = 1$, sest p on 5-st suurem algarv.

Näitame, et kui astendatav p ja moodul m on ühistegurita, peab tsükkel tagasi jõudma elemendini $p^0 \bmod m$. Oletame vastuväiteliselt, et see ei ole nii.

Olgu c esimene jääk, mis esineb teist korda. Siis leiduvad erinevad positiivsed astendajad i ja j nii, et $c \equiv p^i \equiv p^j \bmod m$, aga $p^{i-1} \not\equiv p^{j-1} \bmod m$.

Tähistame $a = p^{i-1} \bmod m$ ja $b = p^{j-1} \bmod m$. Siis saame ekvivalentsi $p^i \equiv p^j \bmod m$ kirjutada kujul

$$a \cdot p \equiv b \cdot p \bmod m\,.$$

See seos tähendab, et $(a \cdot p - b \cdot p) \,\vdots\, m$ ehk $p(a-b) \,\vdots\, m$. Kuna p ja m on ühistegurita, järeldub siit, et $a - b \,\vdots\, m$ ehk $a \equiv b \bmod m$. Saime vastuolu eeldusega, et a ja b on erinevad jäägid mooduli m järgi.

19.10 Selleks, et saada aimu, mis ülesandes toimub, proovime mõned väikesed a väärtused läbi.

Kui $a = 2$, siis saame geomeetrilise jada summa valemist

$$1 + 2 + 2^2 + \ldots + 2^{p-1} = \frac{2^p - 1}{2 - 1} = 2^p - 1\,.$$

Arvutame $2^p - 1$ väärtuse väikeste algarvude p korral, kuni jõuame kordarvuni:

$$2^2 - 1 = 3,\ 2^3 - 1 = 5,\ 2^5 - 1 = 31,\ 2^7 - 1 = 127,\ 2^{11} = 2047 = 23 \cdot 89\,.$$

Niisiis $a = 2$ korral sobib $p = 11$. Kuidas on lugu järgmiste a väärtustega?

Kui $a = 3$, siis $1 + 3^1 = 4$ on kordarv, järelikult sobib $p = 2$.

Kui $a = 4$, siis $1 + 4^1 = 5$ on algarv, aga $1 + 4^1 + 4^2 = 21$ kordarv, järelikult sobib $p = 3$.

Kui $a = 5$, siis $1 + 5^1 = 6$ on kordarv, järelikult sobib $p = 2$.

Kui $a = 6$, siis $1 + 6^1 = 7$ ja $1 + 6^1 + 6^2 = 43$ on algarvud, aga $1 + 6^1 + 6^2 + 6^3 + 6^4 = 1555$ on kordarv, järelikult sobib $p = 5$.

Näeme, et paarituarvulise a korral sobib alati $p = 2$, sest $1 + a$ jagub 2-ga. $a = 4$ puhul aga sobis $p = 3$ ning $a = 6$ puhul $p = 5$.

Siit tekib mõte proovida p rolli mõnda $a - 1$ algtegurit. Kui $a - 1 \,\vdots\, p$, siis $a \equiv 1 \bmod p$. See aga tähendab, et ka $a^2 \equiv 1 \bmod p$, $a^3 \equiv 1 \bmod p$ jne. Järelikult

$$1 + a + a^2 + \ldots + a^{p-1} \equiv \underbrace{1 + 1 + 1 + \ldots + 1}_{p} \equiv 0 \bmod p\,.$$

Kokkuvõttes, kui $a = 2$, saame valida $p = 11$, aga kui $a \geqslant 3$, saame valida p rolli arvu $a - 1$ suvalise algteguri, mis kindlustab, et ülesande avaldis jagub p-ga. Kuna ta on samas p-st suurem, peab tegemist olema kordarvuga.

19.11 Vastus 8.

Ülesande avaldise viimase numbri leidmiseks piisab, kui vaatleme astendatavate viimaseid numbreid (ehk jääke jagamisel 10-ga). Paneme tähele, et kümnendnumbrite järjestikuste astmete leidmisel kehtivad järgmised seaduspärasused:

- numbrite $0, 1, 5$ ja 6 kõik positiivsed täisarvulised astmed lõppevad vastavalt numbritega $0, 1, 5$ ja 6;
- numbri 2 järjestikused positiivsed täisarvulised astmed lõppevad numbritega $2, 4, 6, 8, 2, 4, \ldots$ (tekib tsükkel pikkusega 4);
- numbri 3 järjestikused positiivsed täisarvulised astmed lõppevad numbritega $3, 9, 7, 1, 3, 9, \ldots$ (tekib tsükkel pikkusega 4);
- numbri 4 järjestikused positiivsed täisarvulised astmed lõppevad numbritega $4, 6, 4, 6, \ldots$ (tekib tsükkel pikkusega 2);
- numbri 7 järjestikused positiivsed täisarvulised astmed lõppevad numbritega $7, 9, 3, 1, 7, 9, \ldots$ (tekib tsükkel pikkusega 4);
- numbri 8 järjestikused positiivsed täisarvulised astmed lõppevad numbritega $8, 4, 2, 6, 8, 4, \ldots$ (tekib tsükkel pikkusega 4);
- numbri 9 järjestikused positiivsed täisarvulised astmed lõppevad numbritega $9, 1, 9, 1, \ldots$ (tekib tsükkel pikkusega 2).

Näeme, et moodustuva tsükli pikkus jagab alati arvu 4. Niisiis võime ülesande avaldises asendada astendatavad nende jääkidega jagamisel 10-ga ning astendajad nende jääkidega jagamisel 4-ga. See omakorda tähendab, et jada $a_i = i^i$ liikmete viimased numbrid moodustavad tsükli pikkusega $\text{VÜK}(10, 4) = 20$.

Eraldame jadast $a_1, a_2, \ldots, a_{2011}$ viimased 2000 liiget. Nende viimased numbrid moodustavad 100 tsüklit pikkusega 20. Milline iganes ka ei oleks ühe tsükli arvude summa viimane number, on 100 tsükli arvude viimaste numbrite summa viimane number kindlasti 0.

Järelikult on ülesande avaldise viimane number sama kui summal

$$1^1 + 2^2 + 3^3 + 4^4 + 5^5 + 6^6 + 7^7 + 8^8 + 9^9 + 10^{10} + 11^{11} \equiv$$
$$\equiv 1 + 4 + 7 + 6 + 5 + 6 + 3 + 6 + 9 + 0 + 1 = 48 \equiv 8 \bmod 10\,.$$