Arvuteooria

Kevad 2020

15. praktikumi näidislahendused

1. ülesanne (Urmas Luhaäär ja Kristjan Kallikivi)

Teame, et kui arv n on algarv, siis iga arvu a korral, kus $2 \leq a \leq n-1$, kehtib, et

$$a^{n-1} \equiv 1 \pmod{n}.$$

Anname arvule a suvalisi väärtusi lõigust [2, n-1], et kontrollida, kas n on suure tõenäosusega algarv või mitte. Alati on oht, et tegu on Carmichaeli arvuga. Vaatleme algarve vahemikus [2,20]. Kuna Carmichaeli arvud sisaldavad vähemalt kolme algtegurit, siis on suurem tõenäosus Carmichaeli arvud avastada, võttes a asemele algarvu.

n	2^{n-1}	3^{n-1}	5^{n-1}	7^{n-1}	11^{n-1}	13^{n-1}	17^{n-1}
15841	1	1	1	6790	-	-	-
15871	15212	-	-	-	-	-	-
15881	1	1	1	1	1	1	1

Näeme, et esimesed kaks on kindlasti kordarvud, kuid 15881 on suure tõenäosusega algarv.

Lauri Tart: 15841 oligi Carmichaeli arv.

2. ülesanne (lahenduse autorid on toimetusele teada)

Kõik testitavad arvud on paaritud ning $(2, 15841) = (2, 15871) = (2, 15881) = 1$. Teisendame arvud $n - 1$ ehk $15841 - 1, 15871 - 1, 15881 - 1$ kujule $2^s \cdot t$, kus t on paaritu.

$$15840 = 2^5 \cdot 495$$
$$15870 = 2^1 \cdot 7935$$
$$15880 = 2^3 \cdot 1985$$

Tähistame $t_1 = 495$, $t_2 = 7935$, $t_3 = 1985$.

Uurime, kas 2 on Milleri-Rabini tunnistaja:

n	2^{t_i}	2^{2t_i}	2^{4t_i}	2^{8t_i}	2^{16t_i}
15841	1	1	1	1	1
15871	3592				
15881	-1	1	1		

Seega 15871 on kindlasti kordarv, kuid 15941 ja 15881 võivad olla algarvud, seega uurime nende puhul edasi, kas neil leidub mõni Milleri-Rabini tunnistaja.

Uurime, kas 3 (kuna arvude 15841 ja 15881 ristsummad ei jagu 3-ga, siis $(3, 15841) = (3, 15881) = 1$) on Milleri-Rabini tunnistaja:

n	3^{t_i}	3^{2t_i}	3^{4t_i}	3^{8t_i}	3^{16t_i}
15841	12802	218	1	1	1
15881	8098	4955	-1		

Seega 15841 on kindlasti kordarv, kuid 15881 võib olla algarv, seega kontrollime veel mõne arvu korral, kas sellel arvul leidub on mõni Fermat tunnistaja:

Uurime, kas 5 (seejuures $(5, 15881) = 1$) on Fermat tunnistaja:

n	5^{t_i}	5^{2t_i}	5^{4t_i}
15881	4955	-1	1

Seega 15881 võib olla algarv.

Uurime, kas 7 (seejuures $(7, 15881) = 1$) on Fermat tunnistaja:

n	7^{t_i}	7^{2t_i}	7^{4t_i}
15881	8098	4955	-1

Seega 15881 võib olla algarv.

Kuna katsed leida arvule 15881 Milleri-Rabini tunnistajat ebaõnnestusid täielikult, siis anname siinkohal alla, ja lepime sellega, et 15881 on üsna kindlalt algarv.

3. ülesanne (Erki Külaots ja Marcus Lõo)

Paneme kirja 26 pikkuse tähestiku, et pärast saaks lihtsalt numbreid tähtedeks teha.

1	2	3	4	5	6	7	8	9	10	11	12	13
A	B	C	D	E	F	G	H	I	J	K	L	M
14	15	16	17	18	19	20	21	22	23	24	25	26
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Tükeldame ette antud koodi neljakohalisteks arvudeks. 1400, 5247, 5486 ja 8259. Et saada nendest arvudest dekodeeritud arvud, siis tuleb teha nii

$$\text{arv}^{13} \equiv \text{arv}^8 \cdot \text{arv}^4 \cdot \text{arv} \equiv \text{dekodeeritud} \pmod{9523}$$

Teeme selle läbi iga koodijupi jaoks.

$$\begin{aligned} 1400^2 &\equiv 7785 \pmod{9523} \\ 7785^2 &\equiv 1853 \pmod{9523} \\ 1853^2 &\equiv 5329 \pmod{9523} \\ 1400^{13} &\equiv 5329 \cdot 1853 \cdot 1400 \equiv 0315 \pmod{9523} \end{aligned}$$

$$\begin{aligned} 5247^2 &\equiv 16 \pmod{9523} \\ 16^2 &\equiv 256 \pmod{9523} \\ 256^2 &\equiv 8398 \pmod{9523} \\ 5247^{13} &\equiv 8398 \cdot 256 \cdot 5247 \equiv 2209 \pmod{9523} \end{aligned}$$

$$\begin{aligned} 5486^2 &\equiv 3516 \pmod{9523} \\ 3516^2 &\equiv 1402 \pmod{9523} \\ 1402^2 &\equiv 3866 \pmod{9523} \\ 5486^{13} &\equiv 3866 \cdot 1402 \cdot 5486 \equiv 0400 \pmod{9523} \end{aligned}$$

$$\begin{aligned} 8259^2 &\equiv 7355 \pmod{9523} \\ 7355^2 &\equiv 5385 \pmod{9523} \\ 5385^2 &\equiv 690 \pmod{9523} \\ 8259^{13} &\equiv 690 \cdot 5385 \cdot 8259 \equiv 0109 \pmod{9523} \end{aligned}$$

Seega dekodeeritud sõnum on 0315220904000109. Kasutades üleval toodud tabelit näeme, et sõnum on COVID AI või (loogilisem oleks) COVID 19, kumbki ei lähe kokku originaal digialkirjaga, milleks on SALATÕBI.

Lauri Tart: Võib oletada, et kui allkirjavõltsija suudab muuta allkirjastatud dokumenti nii, et selle uus ja vana sisu on omavahel seotud ja allkiri ikka kehtib, siis ta omab ikkagi õiget salajast võtit ja ei ole võltsija. Teine võimalus on see, et keegi pahatahtlik isik on suutnud dokumendi "COVID 19"või "COVID AI"täiesti juhuslikult (juhusliku äraarvamise eest ei ole ükski süsteem kaitstud) ära allkirjastada. Seda lihtsalt avaliku võtme abil proovides, kas erinevad juhuslikud numbrijadad dekodeeruvad sõnumiks "COVID 19". Tõenäosus et see juhtub on väike, aga mitte olematu. Nüüd siis see äraarvaja saadab igal võimalikul juhul 'allkirjastatud' dokumendi ja loodab, et mõnikord osutub see ka sisuliselt õigeks, nagu näiteks siin ülesandes.

4. ülesanne (Mikael Raihhelgauz ja Maret Sõmer)

Ülesandes antud avalik võti on (93122201, 91), ehk $n = 93122201$, $e = 91$. Leian salajase astendaja d.
Kõigepealt panen tähele, et mooduli n standardkuju on $n = 93122201 = 9511 \cdot 9791$, mis tähendab, et $\varphi(93122201) = 9510 \cdot 9790 = 93102900$.
Seega ringis $\mathbb{Z}_{93102900}$ $\overline{d} = \overline{e}^{-1} = \overline{91}^{-1} = \overline{24554611}$, ehk salajane astendaja $d = 24554611$.

Ülesandes antud kodeeritud sõnumi c dekodeerimiseks (algse sõnumi s leidmiseks) on nüüd vaja leida $c^d \equiv s^{de} \equiv s \pmod{n}$.

Kõigepealt jagan kodeeritud sõnumi
$c = 612342078487902901383160439546899001641242724754789574723$
kaheksanumbrilisteks blokkideks:
61234207, 84879029, 01383160, 43954689, 90016412, 42724757, 89574723.
Nüüd on vaja iga blokk tõsta astmesse d mooduli n järgi. Selleks astendan igat blokki kõigepealt algtegurite 9511 ja 9791 järgi eraldi, ning seejärel kasutan Hiina jäägiteoreemi mooduli n järgi tulemuse leidmiseks.
Hiina jäägiteoreemi kasutamiseks tähistan $m_1 = 9791$, $m_2 = 9511$ ning leian, et ringis $\mathbb{Z}_{9511}$ $\overline{k_1} = \overline{m_1}^{-1} = \overline{9791}^{-1} = \overline{280}^{-1} = 8458$ ning $\mathbb{Z}_{9791}$: $\overline{k_2} = \overline{m_2}^{-1} = \overline{9511}^{-1} = 1084$.
Siis Hiina jäägiteoreemi kohaselt, kui $x \equiv a_1 \pmod{9511}$ ja $x \equiv a_2 \pmod{9791}$, siis $x \equiv a_1 \cdot k_1 \cdot m_1 + a_2 \cdot k_2 \cdot m_2 \pmod{9511 \cdot 9791}$ ehk
$x \equiv a_1 \cdot 8458 \cdot 9791 + a_2 \cdot 1084 \cdot 9511 \pmod{n}$

$61234207^{24554611} \equiv -33 \pmod{9511}$
$61234207^{24554611} \equiv 7005 \pmod{9791}$
$61234207^{24554611} \equiv -33 \cdot 8458 \cdot 9791 + 7005 \cdot 1084 \cdot 9511 \equiv 19050500 \pmod{n}$

$84879029^{24554611} \equiv -1501 \pmod{9511}$
$84879029^{24554611} \equiv 3125 \pmod{9791}$
$84879029^{24554611} \equiv -1501 \cdot 8458 \cdot 9791 + 3125 \cdot 1084 \cdot 9511 \equiv 15140011 \pmod{n}$

$01383160^{24554611} \equiv 341 \pmod{9511}$
$01383160^{24554611} \equiv 5409 \pmod{9791}$
$01383160^{24554611} \equiv 341 \cdot 8458 \cdot 9791 + 5409 \cdot 1084 \cdot 9511 \equiv 09140412 \pmod{n}$

$43954689^{24554611} \equiv 3134 \pmod{9511}$
$43954689^{24554611} \equiv 7298 \pmod{9791}$
$43954689^{24554611} \equiv 3134 \cdot 8458 \cdot 9791 + 7298 \cdot 1084 \cdot 9511 \equiv 01192009 \pmod{n}$

$90016412^{24554611} \equiv 6893 \pmod{9511}$
$90016412^{24554611} \equiv 3813 \pmod{9791}$
$90016412^{24554611} \equiv 6893 \cdot 8458 \cdot 9791 + 3813 \cdot 1084 \cdot 9511 \equiv 00111514 \pmod{n}$

$42724757^{24554611} \equiv -830 \pmod{9511}$

$42724757^{24554611} \equiv 2261 \pmod{9791}$
$42724757^{24554611} \equiv -830 \cdot 8458 \cdot 9791 + 2261 \cdot 1084 \cdot 9511 \equiv 20181512 \pmod{n}$

$89574723^{24554611} \equiv 8417 \pmod{9511}$
$89574723^{24554611} \equiv 1933 \pmod{9791}$
$89574723^{24554611} \equiv 8417 \cdot 8458 \cdot 9791 + 1933 \cdot 1084 \cdot 9511 \equiv 12201519 \pmod{n}$

Seega dekodeeritud tekst on 19050500151400110914041201192009001115142018151212201519.
Loengukonspektis toodud kodeerimise skeemi kohaselt vastavad sellele numbrijadale järgmised tähed:
$19 \mapsto S$, $05 \mapsto E$, $05 \mapsto E$, $00 \mapsto$ " ", $15 \mapsto O$, $14 \mapsto N$, $00 \mapsto$ " ", $11 \mapsto K$,
$09 \mapsto I$, $14 \mapsto N$, $04 \mapsto D$, $12 \mapsto L$, $01 \mapsto A$, $19 \mapsto S$, $20 \mapsto T$, $09 \mapsto I$,
$00 \mapsto$ " ", $11 \mapsto K$, $15 \mapsto O$, $14 \mapsto N$, $20 \mapsto T$, $18 \mapsto R$, $15 \mapsto O$, $12 \mapsto L$,
$12 \mapsto L$, $20 \mapsto T$, $15 \mapsto O$, $19 \mapsto S$.
Järelikult dekodeeritud tekst on "SEE ON KINDLASTI KONTROLLTOS".

5. ülesanne (Mikael Raihhelgauz ja Maret Sõmer)

Diffie-Hellmani võtmevahetuseks on antud tsükliline rühm: $G = \mathbb{Z}^*_{31111123}$ ja selle moodustaja $g = 2$, mis on algjuur mooduli 31111123 järgi. Teine osapool on valinud suvalise naturaalarvu k ning saatnud mulle sõnumi $g^k = 19874654$. Mina valin juhusliku naturaalarvu $l = 666$ ning arvutan $g^{kl} = (g^k)^l$ mooduli 31111123 järgi.

$g^{kl} = (g^k)^l = 19874654^{666} = 19874654^{512} \cdot 19874654^{128} \cdot 19874654^{16} \cdot 19874654^8 \cdot 19874654^2 \equiv$
$\equiv 9328914 \cdot 9372918 \cdot 9452184 \cdot 24146267 \cdot 27339307 \equiv 20612915 \pmod{31111123}$.

Seega (de)kodeerimiseks vajalik sajalane võti on $v = 20612915$. Antud on kodeeritud sõnum $s = 21683015085522922569401525702930015524 97$, ning vaja on leida algne sõnum c. Selleks on antud neljatäheliste blokkidega skeem $c = s - v \pmod{n}$.

Jagan antud sõnumi neljatähelisteks (kaheksanumbrilisteks) blokkideks:
21683015, 08552292, 25694015, 25702930, 01552497.
$c = 21683015 - 20612915 = 01070100$
$c = 08552292 - 20612915 = -12060623 \equiv 19050500 \pmod{31111123}$
$c = 25694015 - 20612915 = 05081100$
$c = 25702930 - 20612915 = 05090015$
$c = 01552497 - 20612915 = -19060418 \equiv 12050705 \pmod{31111123}$

Seega dekodeeritud tekst on 01070100190505000508110005090015120507 05. Loengukonspektis toodud kodeerimise skeemi kohaselt vastavad sellele numbrijadale järgmised tähed: $01 \mapsto A$, $07 \mapsto G$, $01 \mapsto A$, $00 \mapsto$ " ", $19 \mapsto S$, $05 \mapsto E$, $05 \mapsto E$,
$00 \mapsto$ " ", $05 \mapsto E$, $08 \mapsto H$, $11 \mapsto K$, $00 \mapsto$ " ", $05 \mapsto E$, $09 \mapsto I$, $00 \mapsto$ " ",
$15 \mapsto O$, $12 \mapsto L$, $05 \mapsto E$, $07 \mapsto G$, $05 \mapsto E$.
Järelikult dekodeeritud tekst on "AGA SEE EHK EI OLEGE".

Lauri Tart: Kas "OLEGI" asemel "OLEGE" oli viga või meelega selline võetud, jääb lugejale endale ära arvata.

6. ülesanne (lahenduse autorid on toimetusele teada)

Kuna $p \in \mathbb{P}$ ja $p > 5$, siis ilmselt $p \not\equiv 0 \pmod 5$, teiseks kuna $q = 2p - 3 > 7$, siis ka $q \not\equiv 0 \pmod 5$, millest järeldub, et $p \not\equiv 4 \pmod 5$

Kuna avalik võti $(n, 5)$, kus $n = pq$, siis selleks, et võti vastaks RSA tingimustele, peab 5 olema pööratav ringis $\mathbb{Z}_{\phi(n)}$ ehk $(\phi(n), 5) = 1$ ning kuna 5 on algarv, siis see on samaväärne, et $5 \nmid \phi(n)$.

$$\phi(n) = \phi(pq) = (p-1)(q-1) = (p-1)(2p-3-1) = 2p^2 - 6p + 4$$

Ringis $\mathbb{Z}_5$ on polünoomi $2p^2 - 6p + 4$ juurteks $p = 1, 2$, seega kuna $5 \nmid \phi(n)$, siis $p \not\equiv 1, 2 \pmod 5$.

Niisiis jääbki järele ainult üks variant, et $p \equiv 3 \pmod 5$ ning tõesti $(p-1)(q-1) + 1 = 2p^2 - 6p + 4 + 1 \equiv 2 \cdot 3^2 - 6 \cdot 3 + 5 \equiv 18 - 18 \equiv 0 \pmod 5$ ehk $\frac{(p-1)(q-1)+1}{5} \in \mathbb{Z}$.

$$5 \cdot \frac{(p-1)(q-1)+1}{5} = (p-1)(q-1) + 1 = \phi n + 1 \equiv 1 \pmod{\phi n}$$

Nagu näha, siis avaliku ja privaatse võtme korrutis mooduli ϕn järgi on 1, nagu tarvis.

7. ülesanne (Urmas Luhaäär ja Kristjan Kallikivi)

Olgu $n = 2^{2^n} + 1$. Selleks, et 2 ei oleks Fermat' tunnistaja piisab, et $2^{n-1} \equiv 1 \pmod n$, ehk

$$2^{2^{2^n}+1-1} \equiv 2^{2^{2^n}} \equiv 1 \pmod{2^{2^n}+1}.$$

See on samaväärne kongruentsiga

$$2^{2^{2^n}} - 1 \equiv 0 \pmod{2^{2^n}+1}.$$

Hakkame nüüd vasakut poolt tegurdama:

$$2^{2^{2^n}} - 1 \equiv (2^{2^{2^n-1}} + 1)(2^{2^{2^n-1}} - 1) \equiv \cdots \equiv (2^{2^{2^n-1}} + 1) \ldots (2^{2^{2^n-k}} + 1)(2^{2^{2^n-k}} - 1) \equiv \ldots$$

$$(2^{2^{2^n-1}} + 1) \ldots (2^{2^n} + 1)(2^{2^n} - 1) \equiv 0 \pmod{2^{2^n}+1}.$$

Eelviimaseni jõuame, sest iga $k \in \mathbb{N}$ korral $2^k \geq k$.

8. ülesanne (Erki Külaots ja Marcus Lõo)

Teame, et Carmichaeli arvud on paaritud (2 ei saa olla nende algtegur), ruuduvabad ja neil on vähemalt kolm algtegurit (mis on erinevad, sest nad on ruuduvabad). Leiame potentsiaalsed arvud, mis võiks olla Carmichaeli arvud ja mis on väiksemad kui $561 = 3 \cdot 11 \cdot 17$.

$$3 \cdot 5 \cdot 7 \cdot 11 = 1155 > 561$$

$$\begin{aligned}
3 \cdot 5 \cdot 7 &= 105 < 561 \\
3 \cdot 5 \cdot 11 &= 165 < 561 \\
3 \cdot 5 \cdot 13 &= 195 < 561 \\
3 \cdot 5 \cdot 17 &= 255 < 561 \\
3 \cdot 5 \cdot 19 &= 285 < 561 \\
3 \cdot 5 \cdot 23 &= 345 < 561 \\
3 \cdot 5 \cdot 29 &= 435 < 561 \\
3 \cdot 5 \cdot 37 &= 555 < 561 \\
3 \cdot 5 \cdot 41 &= 615 > 561
\end{aligned}$$

$$\begin{aligned}
3 \cdot 7 \cdot 11 &= 231 < 561 \\
3 \cdot 7 \cdot 13 &= 273 < 561 \\
3 \cdot 7 \cdot 17 &= 357 < 561 \\
3 \cdot 7 \cdot 19 &= 399 < 561 \\
3 \cdot 7 \cdot 23 &= 483 < 561 \\
3 \cdot 7 \cdot 29 &= 609 > 561
\end{aligned}$$

$$\begin{aligned}
3 \cdot 11 \cdot 13 &= 429 < 561 \\
3 \cdot 11 \cdot 17 &= 561 = 561
\end{aligned}$$

$$\begin{aligned}
5 \cdot 7 \cdot 11 &= 385 < 561 \\
5 \cdot 7 \cdot 13 &= 455 < 561 \\
5 \cdot 7 \cdot 17 &= 595 < 561 \\
5 \cdot 7 \cdot 19 &= 665 > 561
\end{aligned}$$

$$5 \cdot 11 \cdot 13 = 715 > 561$$

$$7 \cdot 11 \cdot 13 = 1001 > 561$$

Seega peame kontrollima arve $105, 165, 195, 231, 255, 273, 285, 345, 357, 385, 399, 429, 435, 455, 483, 555, 595$.

Kui leidub täisarv a nii, et (a,n) ja $a^{n-1} \not\equiv 1 \pmod{n}$, siis n pole Carmichaeli arv.

	n	105	165	195	231	255	273	285	345	357
2^{n-1}	$\pmod{n}$	46	16	4	67	64	256	196	31	67
	n	385	399	429	435	455	483	555	595	
2^{n-1}	$\pmod{n}$	71	4	256	289	114	466	289	344	

Kuna kõik potentsiaalsed arvud olid paaritud, siis $(n,2) = 1$. Kuna iga n korral näitasime, et $2^{n-1} \not\equiv 1 \pmod{n}$, siis pole arvu, mis oleks Carmichaeli arv ja samas väiksem arvust 561.

Näitame, et 561 on Carmichaeli arv ehk iga a korral kui $(a,561) = 1$, siis $a^{560} \equiv 1 \pmod{561}$.

$$\begin{aligned} a^{560} &= \left(a^{280}\right)^2 \equiv 1 \pmod{3} \\ a^{560} &= \left(a^{56}\right)^{10} \equiv 1 \pmod{11} \\ a^{560} &= \left(a^{35}\right)^{16} \equiv 1 \pmod{17} \end{aligned}$$

Kasutasime Fermat' väikest teoreemi. Kasutades Hiina jäägiteoreemi on lihtne näha, et $a^{560} \equiv 1 \pmod{561}$.

v. Seega 561 on Carmichaeli arv, kusjuures vähim selline.

Lauri Tart: Alternatiiv oleks olnud kasutada sellist abitulemust (lahenduse osa autorid on toimetusele teada):

(Korselti kriteerium) Olgu n ruuduvaba naturaalarv. $a^{n-1} \equiv 1 \pmod{n}$ ja $(a,n) = 1$ $(a \in \mathbb{Z})$ parajasti siis, kui $(p-1) \mid (n-1)$ iga n algteguri p korral.

Tõestus. Piisavus

Olgu p arvu n algtegur ehk $p \mid n$.

Seega kuna $p \mid n$ ja $a^{n-1} \equiv 1 \pmod{n}$, siis ka $a^{n-1} \equiv 1 \pmod{p}$, millest järeldub, et $\phi(p) \mid n-1$ ehk $p-1 \mid n-1$

Tarvilikkus Olgu $n = p_1 \cdot p_2 \dots p_s$, kus $p_i \in \mathbb{P}$ ja kõik algtegurid on paarikaupa erinevad ning $p_i - 1 \mid n-1$.

Vastavalt Fermat' teoreemile $a^{p_i-1} \equiv 1 \pmod{p_1}$, kuna $n-1 = k(p_i-1)$, siis $a^{n-1} \equiv 1 \pmod{p_1}$ Saame kongruentside süsteemi

$$\begin{cases} a^{n-1} \equiv 1 \pmod{p_1} \\ a^{n-1} \equiv 1 \pmod{p_1} \\ \dots a^{n-1} \equiv 1 \pmod{p_s} \end{cases}$$

Hiina jäägiteoreemi kohaselt on sellel üks lahend mooduli $n = p_1 \cdot p_2 \dots p_s$ järgi, seejuures see lahend on $a^{n-1} \equiv 1 \pmod{n}$. □

Lauri Tart: Lemma kasutamine käib nii (Mikael Raihhelgauz ja Maret Sõmer):

Niisiis, $p \in \{3{,}5\}$, $q \in \{5, 7, 11\}$ ja $r \in \{7, 11, 13, 17, 19, 23, 29, 31, 37\}$. Kõigepealt vaatame läbi variandid, kus $p = 3$ ja $q = 5$.

$$3 \cdot 5 \cdot 7 = 105,\ 6 \not| 104; \quad 3 \cdot 5 \cdot 11 = 165,\ 10 \not| 164; \quad 3 \cdot 5 \cdot 13 = 195,\ 4 \not| 194;$$
$$3 \cdot 5 \cdot 17 = 255,\ 16 \not| 254; \quad 3 \cdot 5 \cdot 19 = 285,\ 18 \not| 284; \quad 3 \cdot 5 \cdot 23 = 345, 22 \not| 344;$$
$$3 \cdot 5 \cdot 29 = 435, 4 \not| 434; \quad 3 \cdot 5 \cdot 31 = 465, 30 \not| 464; \quad 3 \cdot 5 \cdot 37 = 555, 36 \not| 554.$$

Kui $p = 3$ ja $q = 7$, siis $6|n - 1 \Rightarrow 3|n - 1$. Aga siis $3 \not| n$, mis on vastuolus asjaoluga $p = 3$. Kui $p = 3$ ja $q = 11$, siis ainus arvust 561 erinev variant on $3 \cdot 11 \cdot 13 = 429$, kuid $10 \not| 428$. Vaatleme juhtu $p = 5$ ja $q = 7$:

$$5 \cdot 7 \cdot 11 = 385, 10 \not| 384; \quad 5 \cdot 7 \cdot 13 = 455, 12 \not| 454; \quad 5 \cdot 7 \cdot 17 = 595 > 561.$$

Jäänud on vaid juht $p = 5$, $q = 11$. Vähim selline arv on $5 \cdot 11 \cdot 13 = 715 > 651$. Niisiis ei leidu arvust 651 väiksemat Carmichaeli arvu.

Lauri Tart: Aga puudu jäi kontroll, et 561 tõesti Korselti kriteeriumit rahuldab (varem kasutasime tarvilikkust, nüüd piisavust):

561 on ruuduvaba ja

$$5 - 1 = 4 \mid 560 = 561 - 1; \quad 11 - 1 = 10 \mid 560 = 561 - 1; \quad 17 - 1 = 16 \mid 560 = 561 - 1.$$