Viðauki C: Talnafræði

Inngangur

Talnafræði, það er fræðin um heilar tölur, hefur í gegnum tíðina verið eitt uppáhalds viðfangsefni margra stærðfræðinga. Haft hefur verið eftir einum fremsta stærðfræðingi sem uppi hefur verið að stærðfræðin væri drottning vísindanna og að talnafræðin væri drottning stærðfræðinnar. Sagan segir svo að ástæðan sem þessi ágæti maður gaf fyrir því að taka talnafræðina fram yfir aðrar greinar stærðfræði hafi verið sú að talnafræðin væri alveg fullkomlega gagnslaus. Kannski kann þetta að hafa verið rétt einu sinni en nú hafa fundist ýmis not fyrir talnafræði, til dæmis þegar upplýsingar eru fluttar yfir á stafrænt form fyrir tölvuvinnslu, í dulmálsfræðum og víðar.

Margar niðurstöður talnafræðinnar má setja fram á þann hátt að allir geti skilið og furðumargt má sanna með aðferðum sem byggja á litlu öðru en menntaskólastærðfræði. Í þessum pistli er ætlunin að kynna grunnatriði talnafræðinnar á óformlegan hátt.

1 Þrepun

Gömul þumalputtaregla segir að ef n kemur fyrir í dæminu þá eigi að leysa það með *þrepun*. Í flest öllum verkefnum tengdum talnafræði þá skýtur n upp kollinum svo vænlegt er að hafa á hreinu hvað þrepun er. Þrepun er nafn á aðferð til að nýta einn af grundvallar eiginleikum náttúrlegra talna:

(†) *Sérhvert ekki tómt mengi af náttúrlegum tölum hefur minnsta stak.*

Til að geta sannað formlega að (†) gildi þá myndum við þurfa að gera formlega grein fyrir náttúrlegu tölunum og eiginleikum þeirra. Margar leiðir eru til að gera þetta en oft er (†) eitt af því sem menn gefa sér í upphafi.

Gerum nú ráð fyrir að við viljum sýna að einhver fullyrðing gildi um allar náttúrlegar tölur sem eru stærri en eða jafnar einhverri gefinni náttúrlegri tölu k. *Lögmálið um stærðfræðilega þrepun* segir að til þess að gera þetta er nóg að sýna að

(i) fullyrðingin gildir um k og

(ii) ef $n \geq k$ og fullyrðingin gildir um n þá gildir hún líka um $n + 1$.

Lítum nú aðeins á hvernig hægt er að réttlæta þetta út frá (†). Gerum ráð fyrir að við höfum framkvæmt (i) og (ii). Ef fullyrðingin okkar gildir ekki um allar náttúrlegar tölur $\geq k$, þá er mengi þeirra náttúrlegra talna $\geq k$ sem hún gildir ekki um ekki tómt. Því hefur þetta mengi minnsta stak sem við

köllum n. Samkvæmt (i) þá er $n > k$. Þar sem n er minnst þeirra náttúrlegu talna sem fullyrðingin gildir ekki um þá vitum við að fullyrðingin gildir um $n-1$. Samkvæmt (ii) þá gildir fullyrðingin um n. Nú er röksemdafærsla okkar komin í hnút vegna þess að í upphafi gerðum við ráð fyrir að fullyrðingin gilti ekki um n. Forsendan um að til væru náttúrlegar tölur $\geq k$ sem fullyrðingin gilti ekki um hlýtur því að hafa verið röng.

Sönnun með þrepun má líkja við að klifra upp stiga. Í skrefi (i) sýnum við að við getum stokkið upp í k-ta þrep stigans og í skrefi (ii) sýnum við að við getum alltaf komist í næsta þrep fyrir ofan . Að þessu tvennu gefnu þá getum við komist í hvaða þrep sem er fyrir ofan k-ta þrepið.

Lítum nú á tvö einföld dæmi um þrepun í framkvæmd.

1.1 Dæmi. Sýnum að fyrir allar náttúrlegar tölur $n \geq 1$ er

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

LAUSN: (i) Fullyrðingin er augljóslega rétt fyrir $n = 1$.

(ii) Gerum nú ráð fyrir að hún sé rétt fyrir eitthvert tiltekið $n \geq 1$. Þetta er oft kallað þrepunarforsenda. Viljum nú sýna að ef reglan hér að ofan gildir um n, þá verði hún einnig að gilda um $n + 1$. En nú er

$$1 + 2 + \cdots + n + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2}$$

og þar með er sannað að reglan okkar gildir fyrir allar náttúrlegar tölur $n \geq 1$.

1.2 Dæmi. Sýnum að fyrir allar náttúrlegar tölur $n \geq 1$ er

$$1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2.$$

LAUSN: (i) Aftur þarf ekkert að gera hér, reglan er augljóslega rétt fyrir $n = 1$.

(ii) Gerum nú ráð fyrir að fullyrðingin gildi fyrir eitthvert tiltekið $n \geq 1$. Þá fáum við að

$$1^3 + 2^3 + \cdots + n^3 + (n+1)^3 = (1 + 2 + \cdots + n)^2 + (n+1)^3.$$

Á hinn bóginn þá sönnuðum við hér að ofan að $2(1+2+\cdots+n) = n(n+1)$ og því er

$$\begin{aligned}
&((1 + 2 + \cdots + n) + (n+1))^2 \\
&\quad = (1 + 2 + \cdots + n)^2 + 2(1 + 2 + \cdots + n)(n+1) + (n+1)^2 \\
&\quad = (1 + 2 + \cdots + n)^2 + n(n+1)(n+1) + (n+1)^2 \\
&\quad = (1 + 2 + \cdots + n)^2 + (n+1)^3,
\end{aligned}$$

sem sýnir að fullyrðingin er einnig rétt fyrir $n+1$.

Oft er þægilegt að nota dálítið sterkari útgáfu af lögmálinu um þrepun, sem við getum kallað *þrepun með breiðri þrepunarforsendu*. Skrefin eru þá að sýna að

(i′) fullyrðingin gildir um k og

(ii′) ef $n \geq k$ og fullyrðingin gildir um $k, k+1, \ldots, n$, þá gildir hún líka um $n+1$.

Þetta má réttlæta á sama hátt og áður út frá (†). Í greininni um frumtölur sjáum við dæmi um þrepun með breiðri þrepunarforsendu.

2 Deilanleiki

Aðal viðfangsefni talnafræðinnar er deilanleiki. Við segjum að heil tala d *gangi upp í* heilu tölunni n, að d sé *þáttur* í n eða að n sé *deilanleg* með d ef til er heil tala k þannig að $n = kd$. Við skrifum þá $d|n$. Til dæmis, þá gildir greinilega fyrir allar heiltölur n að $n|0$ og einnig gildir $1|n$ og $-1|n$. Annað dæmi sem við komum að síðar er að $6|25 \cdot 7^n + 25^n - 32$ fyrir allar náttúrlegar tölur n. Eftirfarandi reglur gilda um deilanleika.

Fyrir allar heilar tölur a, b, c, x og y gildir:

(1) ef $a|b$ og $b|c$ þá er $a|c$;

(2) ef $a|b$ og $a|c$ þá er $a|xb + yc$;

(3) ef $a|b$ og $b|a$ þá er $a = b$ eða $a = -b$;

(4) ef bæði a og b eru náttúrlegar tölur þannig að $b \neq 0$ og $a|b$ þá er $1 \leq a \leq b$.

Til að átta okkur betur á deilanleikahugtakinu þá skulum við fara yfir sönnun á fyrstu reglunni. Það að $a|b$ þýðir að $b = ka$, þar sem k er heil tala. Sömuleiðis er til heil tala j þannig að $c = jb$. En $c = jb = j(ka) = (jk)a$ og okkur hefur þá tekist að skrifa c sem margfeldi af heilli tölu og a svo að $a|c$.

2.1 Dæmi. Sýnum að 13 gangi upp í töluna $4^{2n+1} + 3^{n+2}$ fyrir allar náttúrlegar tölur n.

LAUSN: Beitum þrepun. Byrjum á því að sýna að fullyrðingin sé rétt fyrir $n = 0$. Nú er $4^{2\cdot 0+1} + 3^{0+2} = 4 + 9 = 13$, svo að fullyrðingin er rétt fyrir $n = 0$.

Gerum nú ráð fyrir að fullyrðingin sé rétt fyrir töluna n. Þá gildir $13|4^{2n+1}+3^{n+2}$. En nú er

$$\begin{aligned} 4^{2(n+1)+1}+3^{(n+1)+2} &= 4^{2n+1}\cdot 4^2+3^{n+2}\cdot 3 \\ &= (4^{2n+1}+3^{n+2})\cdot 4^2-3^{n+2}(4^2-3) \\ &= (4^{2n+1}+3^{n+2})\cdot 16-3^{n+2}\cdot 13. \end{aligned}$$

Þrepunarforsenda segir okkar að 13 gangi upp í fyrri liðinn og augljóslega gengur 13 upp í seinni liðinn. Því gildir, samkvæmt reglu 2 hér að ofan, að $13|4^{2(n+1)+1}+3^{(n+1)+2}$. Fullyrðingin er þá rétt fyrir $n+1$ og gildir því fyrir allar náttúrlegar tölur n.

3 Frumtölur

3.1 Skilgreining. *Frumtala er náttúrleg tala p þannig að $p>1$ og engar náttúrlegar tölur aðrar en p og 1 ganga upp í p.*

Fyrstu 15 frumtölurnar eru

$$2,3,5,7,11,13,17,19,23,29,31,37,41,43,47.$$

Frumtölur eru í ákveðnum skilningi, sem lýst er í næstu setningu, byggingarblokkir allra heilla talna, og einnig lykillinn að lausn margra vandamála sem fjalla um deilanleika. Við segjum að tala n sé margfeldi af frumtölum ef til eru frumtölur $p_1,\ldots,p_r$ þannig að $n=p_1\cdot\cdots\cdot p_r$. Hér er leyft að $r=1$, það er að $n=p_1$.

3.2 Setning. *Sérhverja náttúrlega tölu $n\geq 2$ má skrifa sem margfeldi af frumtölum.*

Sönnun 1: Hér beitum við þrepun með breiðri þrepunarforsendu. Fullyrðingin „n er margfeldi af frumtölum“ er greinilega rétt ef $n=2$. Gerum ráð fyrir að fullyrðingin „k er margfeldi af frumtölum“ sé rétt fyrir allar tölur $k=2,\ldots,n$ (þrepunarforsenda) og sýnum að þá er $n+1$ líka margfeldi af frumtölum. Nú er $n+1$ annaðhvort frumtala eða $n+1$ er margfeldi minni náttúrlegra talna k og j. Ef $n+1$ er frumtala þá þurfum við ekki að gera neitt meira í málinu, svo við getum einbeitt okkur að því tilfelli þegar $n+1=kj$ með $2\leq k\leq n$ og $2\leq j\leq n$. Samkvæmt þrepunarforsendu eru bæði k og j margfeldi af frumtölum, segjum $k=p_1\cdot\cdots\cdot p_r$ og $j=p_{r+1}\cdot\cdots\cdot p_s$. En þá er $n+1=kj=p_1\cdot\cdots\cdot p_r\cdot p_{r+1}\cdot\cdots\cdot p_s$, og því er $n+1$ líka margfeldi af frumtölum. Samkvæmt lögmálinu um þrepun með breiðri þrepunarforsendu gildir fullyrðingin „n er margfeldi af frumtölum“ fyrir allar náttúrlegar tölur $n\geq 2$. ■

Sönnun 2: Ef fullyrðingin er röng, þá er mengi náttúrlegra talna $n\geq 2$ sem ekki má skrifa sem margfeldi af frumtölum ekki tómt og hefur því minnsta

stak m. Þá er m ekki frumtala og má því skrifa sem $m = jk$ þar sem j og k eru náttúrlegar tölur minni en m. Þá má skrifa j og k sem margfeldi frumtalna og því einnig m. Við höfum nú leitt þá forsendu að fullyrðingin sé röng til mótsagnar og því hlýtur hún að vera rétt. ■

Við getum reyndar fengið mun skarpari niðurstöðu sem oft er nefnd *undirstöðusetning reikningslistarinnar.*

3.3 Setning. *Sérhverja náttúrlega tölu $n \geq 2$ má rita sem margfeldi af frumtölum með nákvæmlega einum hætti (burtséð frá röð).*

SÖNNUN: Við höfum þegar sýnt að sérhverja tölu $n \geq 2$ má skrifa sem margfeldi af frumtölum. Eftir er að sýna að við getum ekki skrifað n sem margfeldi af frumtölum nema á einn veg, burtséð frá röð. Þetta er ljóst ef $n = 2$. Gerum því ráð fyrir að $n > 2$ og að fullyrðingin sé rétt fyrir allar tölur k þannig að $n > k \geq 2$ (þrepunarforsenda). Gerum einnig ráð fyrir að við höfum skrifað n sem margfeldi af frumtölum á tvo vegu,

$$n = p_1 \cdot \cdots \cdot p_r = q_1 \cdot \cdots \cdot q_s.$$

Með því að breyta röð þáttanna getum við gert ráð fyrir að $p_1 \leq \cdots \leq p_r$ og $q_1 \leq \cdots \leq q_s$. Við fullyrðum að $p_1 = q_1$. Gerum ráð fyrir að til dæmis $p_1 < q_1$. Þá er

$$m = p_1 \cdot q_2 \cdot \cdots \cdot q_s < n$$

og p_1 gengur bæði upp í n og m og því upp í mismuninn $n - m$. Því má skrifa

$$n - m = p_1 \cdot u_1 \cdot \cdots \cdot u_h, \tag{1}$$

þar sem $u_1, \ldots, u_h$ eru frumtölur. Einnig er $n - m = (q_1 - p_1) \cdot q_2 \cdot \cdots \cdot q_s$, og við getum skrifað $q_1 - p_1$ sem margfeldi af frumtölum, $q_1 - p_1 = v_1 \cdot \cdots \cdot v_t$. Þar með er

$$n - m = v_1 \cdot \cdots \cdot v_t \cdot q_2 \cdot \cdots \cdot q_s. \tag{2}$$

En nú er $p_1 < q_1 \leq \cdots \leq q_s$ og talan p_1 gengur ekki upp í $q_1 - p_1$, annars gengi hún líka upp í q_1, sem er fráleitt þar sem q_1 er frumtala. Þar með er p_1 ekki nein af frumtölunum í margfeldinu (2). En þá sýna jöfnurnar (1) og (2) að við höfum skrifað $n - m$ sem margfeldi af frumtölum á tvo ólíka vegu í mótsögn við þrepunarforsendu. Þar með er $p_1 = q_1$. En þá er líka

$$p_2 \cdot \cdots \cdot p_r = q_2 \cdot \cdots \cdot q_s < n,$$

og samkvæmt þrepunarforsendu er $r = s$ og $p_k = q_k$ fyrir $k = 2, \ldots, r$. ■

Eftirfarandi staðreynd er augljós afleiðing af setningu (3.3) og er sönnunin eftirlátin lesandanum.

3.4 Fylgisetning. *Ef frumtala p gengur upp í margfeldi tveggja náttúrlegra talan a og b, þá gengur hún annaðhvort upp í a eða b.* ■

Með þrepun má sanna að ef p er frumtala og $p|a_1 \cdots a_r$ þá er til tala k þannig að $p|a_k$.

Framsetning $n \geq 2$ sem margfeldis

$$n = p_1 \cdots p_r$$

af frumtölum er kölluð *frumþáttun* tölunnar n og tölurnar $p_1, \ldots, p_r$ kallast *frumþættir* hennar. Nú getur frumtalan p_k komið fyrir í margfeldinu oftar en einu sinni, segjum m_k sinnum. Við getum því skrifað

$$n = p_1^{m_1} \cdot p_2^{m_2} \cdots p_s^{m_s},$$

þar sem $p_1, \ldots, p_s$ eru allar ólíkar frumtölur sem koma fyrir í frumþáttun tölunnar n.

3.5 Dæmi. Hvað ganga margar náttúrlegar tölur upp í n?

LAUSN: Tökum eftir að ef $d|n$ þá koma sömu frumtölur og voru í frumþáttun n fyrir í frumþáttun d og ef $d = p_1^{j_1} \cdot p_2^{j_2} \cdot \cdots \cdot p_s^{j_s}$ þá er $0 \leq j_k \leq m_k$ fyrir $k = 1, \ldots, s$. Við getum því fengið allar tölur sem ganga upp í n með því að velja tölurnar j_k. Fyrir hvert j_k þá höfum við $m_k + 1$ möguleika svo að fjöldi náttúrlegra talna sem ganga upp í n er jafn $(m_1 + 1) \cdot (m_2 + 1) \cdot \cdots \cdot (m_s + 1)$.

3.6 Dæmi. Frumþáttið tölurnar (a) 12, (b) 210, (c) $2^{2^5} + 1$, (d) $2^{2^6} + 1$

LAUSN: (a) $12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3^1$.

(b) $210 = 2 \cdot 3 \cdot 5 \cdot 7$. Til gamans skulum við finna hvaða náttúrlegu tölur ganga upp í 210. Þær eru fundnar með því að skoða frumþáttun tölunnar 210. Fáum að tölurnar 1, 2, 3, 5, 6, 7, 10, 14, 15, 21, 30, 35, 42, 70, 105 ,210 eru einu tölurnar sem ganga upp í 210.

(c) $2^{2^5} + 1 = 641 \cdot 6.700.417$.

(d) $2^{2^6} + 1 = 274.117 \cdot 67.280.421.310.721$.

Eitt af því sem menn skemmta sér við er að reyna að finna stórar frumtölur. Franski stærðfræðingurinn Fermat (1601-1665) kom með þá tilgátu að tölurnar $F_n = 2^{2^n} + 1$ væru frumtölur fyrir öll gildi á n, og prófaði þessa tilgátu sína fyrir $n = 1, 2, 3, 4$. Liðir (c) og (d) sýna að F_5 og F_6 eru ekki frumtölur. Reyndar hefur komið í ljós að tilgáta Fermat er langt frá því sanna því að nú hefur tekist að prófa fyrir mörg gildi á $n \geq 5$ hvort F_n er frumtala eða ekki og alltaf komið í ljós að F_n er ekki frumtala.

Nokkur keppni er um það meðal tölvumanna að finna stórar frumtölur og má af og til sjá í blöðum að einhverjum hafi tekist að finna stærri frumtölu en hafi verið þekkt áður. Næsta setning segir okkar að til eru frumtölur hversu stórar sem við viljum.

3.7 Setning. *Til eru óendanlega margar frumtölur.*

Sönnun (Evklíð): Gerum ráð fyrir að einungis séu til endanlega margar frumtölur og köllum þær $p_1, \ldots, p_m$. Setjum

$$q = 1 + p_1 \cdot \cdots \cdot p_m.$$

Þá má skrifa q sem margfeldi af frumtölum. Sér í lagi er til frumtala p sem gengur upp í q. En p getur ekki verið nein af frumtölunum $p_1, \ldots, p_m$ því engin þeirra gengur upp í q. En þetta er mótsögn við að ekki séu til aðrar frumtölur en $p_1, \ldots, p_m$. ■

Það hvernig frumtölurnar dreifast er annað atriði sem hefur verið mikið rannsakað. Til dæmis er vitað að $\frac{n}{\ln n}$ („ln“ táknar náttúrlega lograrn) gefur nokkuð gott mat á því hversu margar frumtölur eru minni en n. Margt er samt ekki vitað; til dæmis er ekki vitað hvort til séu óendanlega margar frumtölur p þannig að $p + 2$ sé líka frumtala.

3.8 Dæmi. Sýnið að $p = 3$ er eina frumtalan þannig að p, $p + 2$ og $p + 4$ eru allt frumtölur.

Lausn: Ljóst er að ef $p = 3$ þá eru tölurnar p, $p + 2$ og $p + 4$ allar frumtölur. Greinilegt er að $p = 2$ kemur ekki til greina. Til að ljúka við dæmið þá þurfum við að sýna að ef $p > 3$ þá er ein talnanna p, $p + 2$, $p + 4$ ekki frumtala. Gerum ráð fyrir að $p > 3$. Ljóst er að 3 gengur upp í einni talnanna $p - 1$, p, $p + 1$ og þar sem p er frumtala sem er stærri en 3 þá er útilokað að $3|p$ svo að annað hvort er $3|p-1$ eða $3|p+1$. Ef $3|p-1$ þá höfum við að $3|p + 2$ og ef $3|p + 1$ þá höfum við að $3|p + 4$.

4 Leifareikningur

4.1 Setning. *Látum m vera heila tölu, $m > 0$. Fyrir sérhverja heila tölu n eru til heilar tölur q og r þannig að*

$$n = qm + r \quad \text{og} \quad 0 \leq r < m.$$

Tölurnar q og r ákvarðast ótvírætt af þessum skilyrðum. Talan r er oft kölluð afgangurinn, eða leifin, þegar við deilum m upp í n.

Sönnun: Ef $n > m$, þá hefur mengið $\{k \in \mathbb{N} : n - km < m\}$ minnsta stak $q \geq 1$. Þá er $n - qm \geq 0$, því annars væri

$$m > n - qm + m = n - (q - 1)m$$

í mótsögn við að $k = q$ sé minnsta talan sem uppfylli ójöfnuna $n - km < m$. Við höfum því að $n = qm + r$ og $0 \leq r < m$ þar sem $r = n - qm$.

Ef hinsvegar $n \leq m$, þá er $2m-n \geq m$ svo við getum notað ofangreint til að rita $2m-n = qm+r$ þar sem $0 \leq r < m$. En þá er $n = (1-q)m+(m-r)$ og $0 < m-r < m$ ef $0 < r < m$ en $n = (2-q)m$ ef $r = 0$. ■

4.2 Setning. *Látum m vera heila tölu, $m > 0$. Fyrir tvær heilar tölur a og b eru eftirfarandi tvö skilyrði jafngild:*

(i) Við fáum sama afgang þegar við deilum m upp í a og þegar við deilum m upp í b.

(ii) $m|a-b$.

Sönnun: Við þurfum að sýna að ef (i) gildir þá gildir (ii) líka og að ef (ii) gildir þá verður (i) að gilda líka.

Ef (i) gildir þá má skrifa $a = q_1m + r$ og $b = q_2m + r$ með $0 \leq r < m$. En þá er $a - b = (q_1 - q_2)m$, svo að $m|a - b$.

Gerum nú ráð fyrir að (ii) gildi. Skrifum $a = q_1m + r_1$ og $b = q_2m + r_2$, þar sem $0 \leq r_1 < m$ og $0 \leq r_2 < m$. Þá er $-m < r_1 - r_2 < m$ eða $|r_1 - r_2| < m$. Við höfum nú $r_1 - r_2 = (a - b) - (q_1 - q_2)m$, og þar sem $m|a-b$ þá er $m|r_1 - r_2$ svo til er heil tala z þannig að $r_1 - r_2 = zm$. En þá er $m > |r_1 - r_2| = |z|m$ og því $1 > |z|$ svo að $z = 0$ og þá er $r_1 = r_2$. Við fáum því sama afgang þegar við deilum m í a og þegar við deilum m í b. ■

4.3 Skilgreining. *Látum m vera heila tölu, $m > 0$. Við segjum að heilar tölur a og b séu samleifa með tilliti til m og skrifum*

$$a \equiv b \pmod{m}$$

ef við fáum sama afgang hvort sem við deilum m upp í a eða b, það er að segja ef $m|a - b$.

Ljóst er að fyrir sérhverja heila tölu a gildir $a \equiv a \pmod{m}$ og einnig að ef a og b eru heilar tölur þannig að $a \equiv b \pmod{m}$ þá gildir líka að $b \equiv a \pmod{m}$. Heilu tölurnar skiptast upp í m flokka eftir því hvaða afgang við fáum þegar við deilum upp í þær með m. Við köllum þessa flokka *leifaflokka* með tilliti til m. Ef til dæmis $m = 2$ þá eru leifaflokkarnir tveir, nefnilega mengi allra sléttra talna og hins vegar mengi allra oddatalna.

4.4 Setning. *Látum m vera heila tölu stærri en núll.*

(a) Fyrir allar heilar tölur a, b, c gildir að ef $a \equiv b \pmod{m}$ og $b \equiv c \pmod{m}$ þá er $a \equiv c \pmod{m}$.

(b) Ef a, b, c, d eru heilar tölur, n er náttúrleg tala og

$$a \equiv b \pmod{m}, \quad c \equiv d \pmod{m}$$

þá gildir að

$$\begin{aligned} a+c &\equiv b+d \pmod m \\ a-c &\equiv b-d \pmod m \\ ac &\equiv bd \pmod m \\ a^n &\equiv b^n \pmod m. \end{aligned}$$

(c) Ef a, b eru heilar tölur þannig að $a \equiv b \pmod m$ og d er heil tala þannig að $d > 0$ og $d|m$ þá gildir $a \equiv b \pmod d$.

Sönnun: (a) Ef m gengur upp í $a-b$ og $b-c$ þá gengur m líka upp í $a-c = (a-b)+(b-c)$.

(b) Ef m gengur upp í $a-b$ og $b-c$ þá gengur m líka upp í sérhverri talnanna

$$\begin{aligned} (a+c)-(b+d) &= (a-b)+(c-d) \\ (a-c)-(b-d) &= (a-b)-(c-d) \\ ac-bd &= (a-b)c+b(c-d). \end{aligned}$$

Síðasta atriðið í lið (b) má svo fá með þrepun yfir n með því að nota næst síðasta atriðið.

(c) Ef $d|m$ og $m|a-b$ þá gildir $d|a-b$. ■

4.5 Dæmi. Sýnum að $6|25 \cdot 7^n + 25^n - 32$.

Lausn: Höfum að $25 \equiv 1 \pmod 6$ og $7 \equiv 1 \pmod 6$ og $32 \equiv 2 \pmod 6$. Notum nú síðustu setningu til að reikna afganginn þegar við deilum 6 upp í $25 \cdot 7^n + 25^n - 32$. Fáum þá að

$$25 \cdot 7^n + 25^n - 32 \equiv 1 \cdot 1^n + 1^n - 2 \equiv 1 + 1 - 2 \equiv 0 \pmod 6.$$

Svo að $6|25 \cdot 7^n + 25^n - 32$.

4.6 Dæmi. Sýnum að $7|24^5 + 11^5$.

Lausn: Höfum að $24 \equiv 3 \pmod 7$ og að $11 \equiv 4 \pmod 7$ en hér er hentugra að nota aðra jöfnu, $11 \equiv -3 \pmod 7$. Þá er

$$24^5 + 11^5 \equiv 3^5 + (-3)^5 \equiv 0 \pmod 7.$$

(Athugið að þetta dæmi má einnig leysa á annan hátt.)

Nú er það þekkt að sérhverja náttúrlega tölu n má rita ótvírætt í tugakerfi. Það þýðir að til eru tölur $a_k \in \{0, 1, \ldots, 9\}$ þannig að $n = \sum_{k=0}^{m} a_k 10^k$. Töluna $\sum_{k=0}^{m} a_k$ köllum við *þversummu* tölunnar n. Þannig er til dæmis þversumma tölunnar 269 talan $2+6+9 = 17$.

4.7 Setning. *(a) Önnur talnanna 3 eða 9 gengur upp í tölu n þá og því aðeins að hún gangi upp í þversummu n.*

(b) Talan 11 gengur upp í tölu $n = \sum_{k=0}^{m} a_k 10^k$ þá og því aðeins að 11 gangi upp í tölunni $\sum_{k=0}^{m}(-1)^k a_k = a_0 - a_1 + a_2 - \cdots + (-1)^n a_n$.

(c) Önnur talnanna 2 eða 5 gengur upp í tölu n þá og því aðeins að hún gangi upp í síðasta tölustaf n.

(d) Talan 4 gengur upp í tölu n þá og því aðeins að 4 gangi upp í $2a_1 + a_0$ þar sem a_0 er talan í einingasæti n og a_1 talan í tugasæti n.

SÖNNUN: Setningin er bein afleiðing af eftirfarandi jöfnum:

$$\sum_{k=0}^{m} a_k 10^k \equiv \sum_{k=0}^{m} a_k \pmod 3 \tag{a}$$

$$\sum_{k=0}^{m} a_k 10^k \equiv \sum_{k=0}^{m} a_k \pmod 9 \tag{a$'$}$$

$$\sum_{k=0}^{m} a_k 10^k \equiv \sum_{k=0}^{m} (-1)^k a_k \pmod{11} \tag{b}$$

$$\sum_{k=0}^{m} a_k 10^k \equiv a_0 \pmod 2 \tag{c}$$

$$\sum_{k=0}^{m} a_k 10^k \equiv a_0 \pmod 5 \tag{c$'$}$$

$$\sum_{k=0}^{m} a_k 10^k \equiv 2a_1 + a_0 \pmod 4. \tag{d}$$

■

Leifareikningur er mjög gott tæki til að fást við talnafræði. Við munum láta hér staðar numið en sem dæmi um það sem má sanna með þeim tækjum sem við höfum byggt upp eru eftirfarandi setningar. Sú fyrri er oft mjög hjálpleg við lausn dæma.

4.8 Setning. (Litla Fermat-setningin) *Látum p vera frumtölu og a vera heiltölu þannig að p gangi ekki upp í a. Þá er*

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

Þetta má einnig orða þannig að fyrir allar heilar tölur n gildir að $p | n^p - n$.

4.9 Setning. (Wilson) *Fyrir sérhverja frumtölu p gildir að*

$$(p-1)! \equiv -1 \pmod p.$$