Od pismenoga dijeljenja do Fermatovog maloga teorema

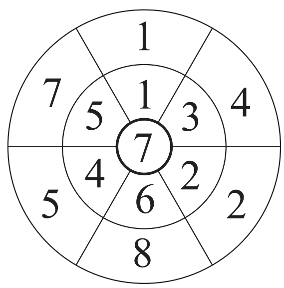
ZVONIMIR ŠIKIĆ, Zagreb

Kada prirodni broj pismeno dijelimo nekim drugim prirodnim brojem, kao rezultat najčešće dobijemo opći decimalni broj s beskonačno mnogo decimala koje se periodički ponavljaju. Na primjer,

$$
\begin{array}{l}
2 : 3 = 0.666\ldots = 0.\overline{6} \\
20 \\
\;\;20 \\
\;\;\;\;20 \\
\;\;\;\;\;\;\ddots
\end{array}
$$

Nešto složeniji primjer je

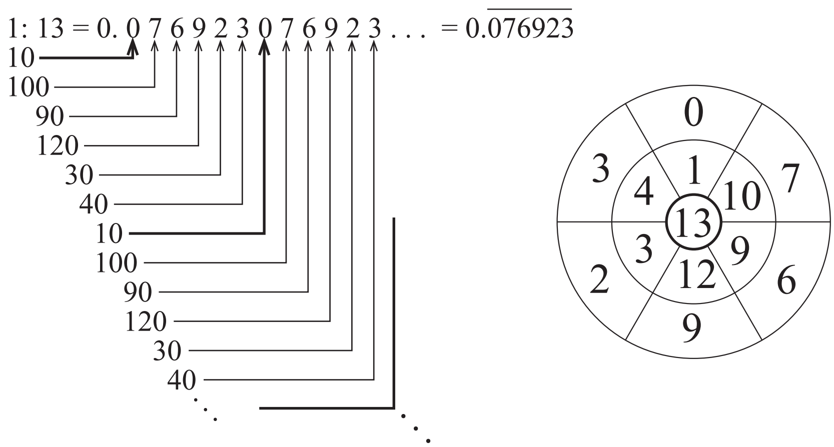
$$
\begin{array}{l}
1 : 7 = 0.\,1\;4\;2\;8\;5\;7\;1\;4\;2\;8\;5\;7\;\ldots = 0.\overline{142857} \\
10 \\
\;\;30 \\
\;\;\;\;20 \\
\;\;\;\;\;\;60 \\
\;\;\;\;\;\;\;\;40 \\
\;\;\;\;\;\;\;\;\;\;50 \\
\;\;\;\;\;\;\;\;\;\;\;\;10 \\
\;\;\;\;\;\;\;\;\;\;\;\;\;\;30 \\
\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;20 \\
\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;60 \\
\;40 \\
\;50 \\
\;\ddots
\end{array}
$$



Decimale 1, 4, 2, 8, 5, 7 dobiju se tako da se brojevi 1, 3, 2, 6, 4, 5 uzastopno dijele brojem 7. Budući da se ta dijeljenja ciklički ponavljaju, preglednije ih prikazujemo u rozeti. U njenom središtu istaknut je broj kojim se dijeli (u ovom slučaju 7). U nutarnjem vijencu istaknuti su brojevi koji se dijele (u ovom slučaju 1, 3, 2, 6, 4, 5), a u vanjskom vijencu su rezultati tih dijeljenja (u ovom slučaju 1, 4, 2, 8, 5, 7). Koristeći se rozetom neposredno možemo ispitati rezultate svih ostalih dijeljenja oblika $n : 7$, za $n < 7$. (To su decimalni zapisi racionalnih brojeva oblika $n/7$, za $n < 7$.) Na primjer,

$$5/7 = 0.\overline{714285}, \qquad 6/7 = 0.\overline{857142}.$$

Pokušajmo sada konstruirati odgovarajuću rozetu za dijeljenja s 13 polazeći od osnovnog dijeljenja $1 : 13$.



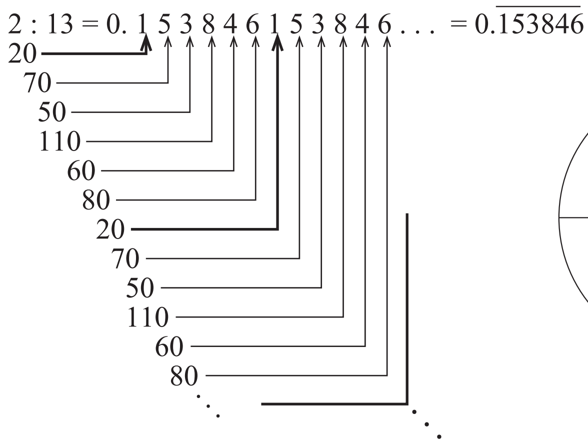
Dobivena rozeta omogućava neposredni ispis decimalnih razvoja sljedećih razlomaka:

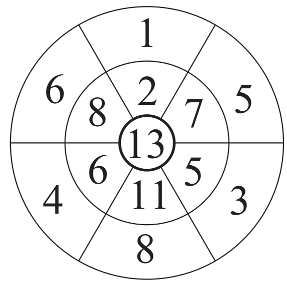
$$1/13, \quad 10/13, \quad 9/13, \quad 12/13, \quad 3/13 \quad \text{i} \quad 4/13.$$

Na primjer,

$$9/13 = 0.\overline{692307}, \qquad 4/13 = 0.\overline{307692}.$$

Međutim, to je samo polovica od svih razlomaka oblika $n/13$, za $n < 13$. Drugu polovicu "pokriva" rozeta koju nalazimo provođenjem jednog od preostalih dijeljenja, npr.

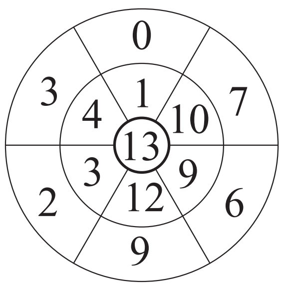


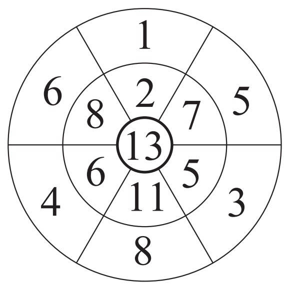


Iz nje možemo neposredno odčitati decimalne razvoje preostalih razlomaka. Na primjer,

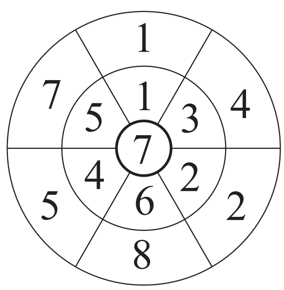
$$5/13 = 0.\overline{384615}, \qquad 8/13 = 0.\overline{615384}.$$

Rezimirajmo. Decimalni zapisi razlomaka $n/13$, za $n < 13$, potpuno su određeni sa sljedeće 2 rozete duljine 6.



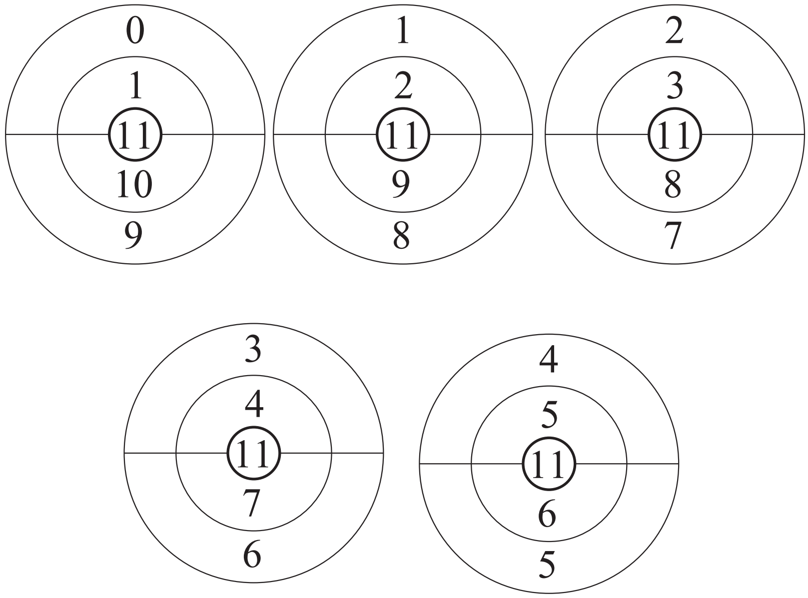


Na isti su način decimalni zapisi svih razlomaka oblika $n/7$, za $n < 7$, bili potpuno određeni sa sljedećom rozetom duljine 6.



Zadatak 1.

Provedite 5 odgovarajućih dijeljenja i provjerite da sljedećih 5 rozeta duljine 2 potpuno određuje decimalne zapise svih razlomaka oblika $n/11$ (za $n < 11$).



Zadatak 2.

Nađite rozete koje određuju decimalne zapise razlomaka oblika $n/21$, za $n < 21$.
(Uputa: Trebali biste dobiti 3 rozete duljine 6 i 2 duljine 1.)

Zadatak 3.

Što možete reći o rozetama za razlomke oblika:

a) $n/3$ ($n < 3$), b) $n/9$ ($n < 9$),
c) $n/6$ ($n < 6$), d) $n/5$ ($n < 5$).

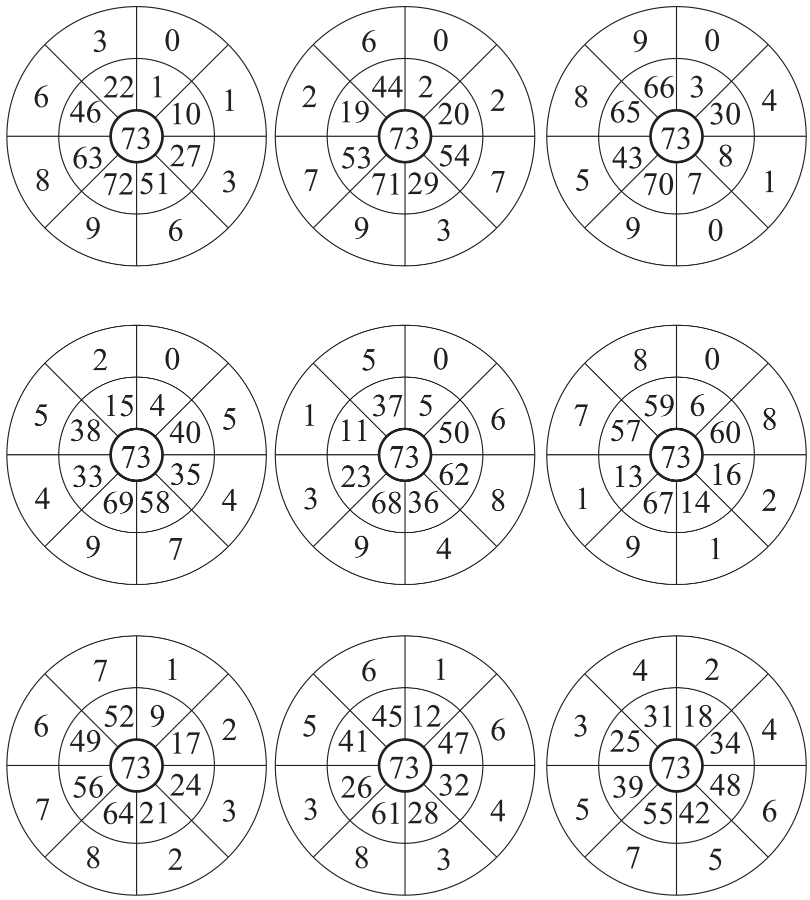
Zadatak 4.

Izračunajte rozete za razlomke oblika:

a) $n/17$ ($n < 17$), b) $n/31$ ($n < 31$),
c) $n/37$ ($n < 37$), d) $n/53$ ($n < 53$).

Zadatak 5.

Provedite 9 odgovarajućih dijeljenja i provjerite da su decimalni zapisi razlomaka oblika $n/73$ $(n < 73)$ opisani sa sljedećih 9 rozeta duljine 8.



Zadatak 6.

Provodeći odgovarajuća dijeljenja (možete se poslužiti i kalkulatorom) pokažite da su decimalni zapisi razlomaka oblika $n/231$ $(n < 231)$ određeni rozetama duljine 1, 2 i 6. (Kraće kažemo da broju 231 pripadaju rozete duljine 1, 2 i 6.)

Ako ste riješili prethodne zadatke, sigurno ste uočili da prostim brojevima p koji ne dijele dekadsku bazu 10 pripadaju rozete konstantne duljine l_p. Na primjer, $l_3 = 1$, $l_7 = 6$, $l_{11} = 2$, $l_{17} = 16$, $l_{31} = 15$, $l_{37} = 3$, $l_{53} = 13$ i $l_{73} = 8$. S druge strane, složeni brojevi mogu imati rozete različitih duljina. Broj 21 iz 2. zadatka ima rozete duljine 6 i 1, što su duljine koje odgovaraju njegovim djeliteljima 7 i 3. Broj

231 iz 6. zadatka, ima rozete duljine 6, 2 i 1, što su duljine koje odgovaraju njegovim djeliteljima 7, 11 i 3. Ukratko, duljine rozeta koje pripadaju nekom broju zapravo su duljine rozeta koje pripadaju njegovim prostim faktorima. Dokaz ove činjenice prepuštamo čitatelju, a mi ćemo dokazati da prostom broju p (koji ne dijeli dekadsku bazu 10) pripadaju rozete jedne jedine duljine l_p.

Naime, duljine rozeta koje pripadaju prostom broju p (a koji ne dijeli bazu 10) jesu duljine periodičkih blokova u decimalnim zapisima razlomaka n/p. Ono što trebamo dokazati jest da su te duljine iste za svaki n. To pak slijedi iz banalne činjenice da zbrajanjem periodičkih blokova istih duljina ne možemo dobiti periodičke blokove veće duljine. Dakle, blok koji odgovara razlomku n/p nije veći od bloka koji odgovara razlomku $1/p$, jer je

$$\frac{n}{p} = \underbrace{\frac{1}{p} + \frac{1}{p} + \ldots + \frac{1}{p}}_{n \text{ puta}}$$

S druge strane, ni blok koji odgovara razlomku $1/p$ nije veći od bloka koji odgovara razlomku n/p, jer je

$$\frac{1}{p} = \underbrace{\frac{n}{p} + \frac{n}{p} + \ldots + \frac{n}{p}}_{m \text{ puta}} - k,$$

za neki cijeli k. Naime, iz činjenice da je p prost slijedi da postoji m takav da je $mn \equiv 1 \pmod p$. No, to znači da je $mn - kp = 1$ za neki cijeli k, iz čega se gornja jednakost dobiva dijeljenjem s p.

Sjetimo se još jednom što je zapravo l_p. To je duljina periodičkog bloka u decimalnom zapisu razlomka $1/p$, tj. l_p je najmanji prirodni broj takav da je

$$(1) \qquad 10^{l_p} \cdot \frac{1}{p} - \frac{1}{p} \in \boldsymbol{N}$$

Na primjer,

$$10^6 \cdot \frac{1}{7} - \frac{1}{7} = 10^6 \cdot 0.\overline{142857} - 0.\overline{142857} =$$
$$= 142857.\overline{142857} - 0.\overline{142857} = 142857 \in \boldsymbol{N}.$$

No (1) zapravo znači da je

$$(2) \qquad 10^{l_p} \equiv 1 \pmod p,$$

tj. l_p je najmanji prirodni broj takav da vrijedi (2).

S druge strane primijetimo da ukupno r_p rozeta duljine l_p potpuno i jednoznačno opisuje $p-1$ razlomaka oblika n/p (za $n<p$ i $p \nmid 10$), pa je zato

$$r_p \cdot l_p = p - 1. \tag{3}$$

(Na primjer, u 4. zadatku je a) $1 \cdot 16 = 17 - 1$, b) $2 \cdot 15 = 31 - 1$, c) $12 \cdot 3 = 37 - 1$ i d) $4 \cdot 13 = 53 - 1$, dok je u 5. zadatku $9 \cdot 8 = 73 - 1$.) Iz (2) i (3) slijedi da za svaki prosti p koji ne dijeli 10 vrijedi:

$$10^{p-1} \equiv 1 \pmod{p}. \tag{4}$$

Da smo sva naša razmatranja proveli za zapise u bazi b, umjesto za decimalne zapise u bazi 10, došli bismo do zaključka da vrijedi Fermatov mali teorem.

FERMATOV MALI TEOREM

Za svaki prosti p koji ne dijeli b

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