Tok zavesti: teoretskoštevilske funkcijske enačbe

Luka Urbanc (luka.urbanc24@gmail.com)

21. november 2025

1 Uvodni

Naloga 1.1

Najdi vse $f\colon \mathbb{Z} \to \mathbb{Z}$, za katere $f(2a) + 2f(b) = f(f(a+b))$ za vse $a, b \in \mathbb{Z}$.

Dokaz. Najprej neumnosti: iz $(0, b)$, $(a, 0)$ sledi $f(0) + 2f(b) = f(f(b))$ in $f(2a) + 2f(0) = f(f(a))$.

To združimo, da se znebimo $f(f(x))$ in takoj dobimo aditivnost, s čimer zaključimo po Cauchyjevi enačbi. □

Naloga 1.2

Najdi vse $f\colon \mathbb{N} \to \mathbb{N}$, za katere velja $m^2 + f(n) \mid mf(m) + n$ za vse $m, n \in \mathbb{N}$.

Dokaz. Najprej neumnosti: z vstavljanjem enk dobimo $1 + f(n) \mid f(1) + n$ in $m^2 + f(1) \mid mf(m) + 1$. Iz tega sledi $m^2 + f(1) \leq mf(m) + 1$, zato $m \leq f(m)$.

V iskanju poenostavitev vstavimo še $m = f(n)$, torej $f(n) \mid n$. Sedaj imamo $f(n) \leq n$ in $m \leq f(m)$, torej $f(n) = n$. □

2 Malo bolj teoretskoštevilske

Naloga 2.1

Naj bo $\mathbb{P}$ množica vseh praštevil. Določi vse funkcije $f : \mathbb{P} \to \mathbb{P}$, za katere velja

$$f(p)^{f(q)} + q^p = f(q)^{f(p)} + p^q$$

za vse $p, q \in \mathbb{P}$.

Dokaz. $q = 2$ da $f(p)^{f(2)} + 2^p = f(2)^{f(p)} + p^2$. Splača se nam uporabljati parnost praštevil: iz parnosti $f(2)$ lahko izrazimo parnost $f(p)$. Če je $f(2)$ lih, je $f(p)$ sod za vse lihe p, torej $f(p) = 2$ za vse lihe p, kar ne more biti. Torej je $f(2)$ sod (enak 2) in $f(p)$ lih za vse lihe p.

Iz začetne enačbe sedaj sledi $f(p)^2 + 2^p = 2^{f(p)} + p^2$. Če preuredimo, dobimo $2^p - p^2 = 2^{f(p)} - f(p)^2$. Idejno funkcija $2^n - n^2$ raste dovolj hitro, da je injektivna, kar bi nam dalo $f(p) = p$ za vsa praštevila p. Z lahkoto se prepričamo, da zares strogo raste za $n \geq 4$, $2^2 - 2^2 = 0$ pa se tudi ne ujema z ostalimi vrednostmi na praštevilih. S tem zaključimo. □

Naloga 2.2

Določi vse $f\colon \mathbb{N} \to \mathbb{N}$, za katere velja $f(a) + b \mid a^2 + f(a)f(b)$ za vse $a, b \in \mathbb{N}$.

Dokaz. Neumnosti: $1, 1$ nam da $f(1) + 1 \mid 1 + f(1)^2$ oz. $f(1) + 1 \mid 2$ oz. $f(1) = 1$. Iz tega dobimo $f(a) + 1 \mid a^2 + f(a)$ in $1 + b \mid 1 + f(b)$. Iz prvega dobimo $f(a) + 1 \mid a^2 - 1$, iz drugega pa $b \leq f(b)$. To ni dovolj.

Še zadnja (glavna) neumnost: a, a da $f(a) + a \mid a^2 + f(a)^2$, torej $f(a) + a \mid 2a^2$ (znebimo se neznanega na desni strani).

To nam da največ, če je a praštevilo. Sledi $f(p) + p \in \{1, 2, p, 2p, p^2, 2p^2\}$. Prve tri niso možne, zadnja tudi ne (iz $f(a) + 1 \mid a^2 - 1$). Ostane $f(p) + p = p^2$ ali $f(p) + p = 2p$, torej $f(p) = p^2 - p$ ali $f(p) = p$.

Da ovržemo prvo, uporabimo kako izmed neumnosti: $1 + p \mid 1 + f(p)$ da $1 + p \mid p^2 - p + 1$, ekvivalentno $p + 1 \mid 3$, kar je možno samo za $p = 2$. A tam sta obe možnosti, p in $p^2 - p$, enaki!

Zdaj imamo $f(p) = p$ za vsako praštevilo p. Sledi $f(a) + p \mid a^2 + pf(a)$ in $p + b \mid p^2 + pf(b)$. Iz drugega za dovolj velike p sledi (ker sta p in b tuja) $p + b \mid p + f(b)$. To pa izgleda nemogoče, natančneje $p + b \mid f(b) - b$ torej $f(b) = b$. □

Naloga 2.3

Določi vse $f\colon \mathbb{N} \to \mathbb{N}$, za katere velja $f(f(x)f(y)) = xy$ in $f(2025x + 1) = 2025x + 1$ za vse naravne x, y.

Dokaz. Neumnosti: $y = 1$ da $f(f(x)f(1)) = x$. To pomeni, da je f bijekcija. Krajši premislek pokaže, da iz tega sledi $f(1) = 1$, saj bi v nasprotnem $f(f(x)f(1))$ pokril samo del naravnih števil.

Sedaj imamo $f(f(x)) = x$. To izkoristimo tako, da vstavimo $f(x), f(y)$ v začetno enačbo, kar da $f(xy) = f(f(f(x))f(f(y))) = f(x)f(y)$. Torej je f multiplikativna funkcija, ki je hkrati involucija (to je ekvivalentno 1. pogoju).

Zdaj uporabimo še pogoj $f(2025x + 1) = 2025x + 1$. Multiplikativne funkcije so določene s svojimi vrednostmi na praštevilih. Ali lahko iz 2. pogoja dobimo vrednost na praštevilu?

Opazimo, da če $p \nmid 2025$, potem je po malem Fermatu neka potenca $p^k \equiv 1 \pmod{2025}$. Torej obstaja tak x, da je $2025x + 1 = p^k$. Iz 2. pogoja sledi $f(p^k) = p^k$, torej $f(p) = p$ za vsako praštevilo, ki ne deli 2025. Zanimajo nas še $f(3)$ in $f(5)$. Tu nam pride prav dejstvo, da je f involucija, torej $f(f(3)) = 3$ in $f(f(5)) = 5$. Sledi, da $f(3)$ in $f(5)$ nista deljiva

s praštevili, različnimi od 3 in 5. Torej sta lahko le zmnožka potenc teh praštevil. Če je $f(3) = 3^a5^b$ in $f(5) = 3^c5^d$, pa iz involucije sledi $3 = f(3^a5^b) = f(3)^a f(5)^b = 3^{a^2+bc}5^{ab+bd}$ in $5 = f(3^c5^d) = f(3)^c f(5)^d = 3^{ac+dc}5^{bc+dd}$. Reševanje teh enačb v naravnih številih da $f(3) = 3$ in $f(5) = 5$, ali pa $f(5) = 3$ in $f(3) = 5$. □

Naloga 2.4

Najdi vse funkcije $f\colon \mathbb{N} \to \mathbb{N}$, za katere velja $a + f(b) \mid a^2 + bf(a)$ za vse $a, b \in \mathbb{N}$ z $a + b > 2025$.

Dokaz. Tu iz neumnosti ne dobimo veliko. Lahko pa bi si zaželeli, da je desna stran praštevilo, saj nam b ponuja veliko svobode. Na pamet nam pade Dirichletov izrek o praštevilih v aritmetičnih zaporedjih, ki pravi, da je v množici števil oblike $kn + m$ za tuji k in m neskončno mnogo praštevil. Ker želimo, da sta a in $f(a)$ tuja, je smiselno vzeti $a = 1$. Tako dobimo $1 + f(b) \mid 1 + bf(1)$ in je za neskončno mnogo velikih b desna stran praštevilo. Torej mora biti $1 + f(b) = 1 + bf(1)$ za neskončno mnogo velikih b, kar pomeni, da je $f(b) = bf(1)$ za vse te b. Če to vstavimo v začetno enačbo, dobimo $a + kb \mid a^2 + kab = a(a + kb)$, kar deluje. □

Naloga 2.5

Naj bo $n \geq 1$ liho naravno število. Določi vse funkcije $f\colon \mathbb{Z} \to \mathbb{Z}$, za katere $f(x) - f(y)$ deli $x^n - y^n$ za vse $x, y \in \mathbb{Z}$.

Dokaz. Prva opazka: f je injektivna. Druga: če deluje f, deluje tudi $f + c$, zato BŠS vzamemo $f(0) = 0$. Sedaj vstavimo $y = 0$, kar da $f(x) \mid x^n$ za vse x, kar pomeni $f(1) = \pm 1$. Spet za poenostavitev vzamemo $f(1) = 1$, saj drugače vzamemo $-f$. Podobno dobimo $f(-1) = \pm 1$, in $f(1) - f(-1) \mid 2$, zato $f(-1) - 1$. Sledi $f(x) - 1 \mid x^n - 1$ in $f(x) + 1 \mid x^n + 1$ za vse x.

Najbolj preprosta enačba, ki jo imamo, je $f(x) \mid x^n$. Vanjo se splača vstaviti p, kar nam da $f(p) = \pm p^d$, kjer je $d \in \{1, \ldots, n\}$ (0 ni, ker imamo injektivnost). Znebimo se še minusa. $f(p) = -p^d$ bi pomenilo $-p^d - 1 \mid p^n - 1$ in $-p^d + 1 \mid p^n + 1$. Pri takih deljivostih nam pride prav Evklidov algoritem, ki nam da $n = qd + r$ z $0 \leq r < d$. Iz druge deljivosti tako dobimo $p^d - 1 \mid p^r + 1$. A ker $p^r + 1 \leq p^{d-1} + 1 < p^d - 1$ za $p > 2$, dobimo protislovje za lihe p.

Zanje torej velja $f(p) = p^d$, kjer je d nek lihi delitelj n, odvisen od p.

Vstavimo to v enačbo: $f(x) - p^d \mid x^n - p^n$. Kot ponavadi, skušamo na desni ali dobiti praštevilo ali pa nekaj majhnega. Tu se izkaže, da želimo nekaj majhnega. Deljivost je namreč ekvivalentna $f(x) - p^d \mid (x^n - p^n) - (f(x)^{n/d} - p^n) = x^n - f(x)^{n/d}$. Če pošljemo p v neskončnost, na levi strani dobimo neko veliko število (po absolutni vrednosti večje od $p - f(x)$), na levi pa nekaj omejenega (kvečjemu $|x|^n + |f(x)|^n$ po absolutni vrednosti), kar pomeni, da je za vsa dovolj velika praštevila (taka, da $p > f(x)$ in $p - f(x) > |x|^n + |f(x)|^n$) edina možnost to, da $x^n = f(x)^{n/d}$ in $f(x) = x^d$. Iz tega dobimo še to, da so d enaki za vsa praštevila, saj drugače ne bi dobili enake vrednosti $f(x)$ za različna praštevila p. Sledi, da je $f(x) = x^d$ za vsa naravna števila x.

Da dobimo končni odgovor, ne smemo pozabiti na $\pm$ in $+c$. Tako je končni odgovor $f(x) = \pm x^d + c$ za neko konstanto c in neko liho deliteljico d števila n. □

Naloga 2.6

Najdi vse funkcije $f\colon \mathbb{N} \to \mathbb{N}$, za katere velja $f(ab) = f(a)f(b)$ in $a+b \mid f(a)+f(b)$ za vse $a, b \in \mathbb{N}$.

Dokaz. Neumnosti: kot pri vseh multiplikativnih funkcijah imamo tu zastonj dano $f(1) = 1$. Vstavimo $b = 1$, kar da $a+1 \mid f(a)+1$. Vstavimo še $b = a$, kar da $a \mid f(a)$.

Da naredimo kaj konkretnejšega, poskusimo izkoristiti multiplikativnost. Nad eno samo vrednostjo lahko dobimo več kontrole le s potenciranjem. Vstavimo torej a^k v $a+1 \mid f(a)+1$, kar da $a^k+1 \mid f(a^k)+1 = f(a)^k+1$. Pri takih enačbah je najbolj koristno na levi strani poskusiti sforsirati nek praštevilski delitelj z uporabo malega Fermatovega izreka. Če je p praštevilo, ki ne deli a, obstaja k, da $a^k \equiv 1 \pmod{p}$. Torej $p \mid a^k - 1 \ldots$ V resnici imamo težavo, saj je izraz v enačbi oblike $a^k + 1$, ne $a^k - 1$. Kako to popraviti?

Želeli bi seveda vstaviti -1 namesto 1, a tega žal ne moremo narediti dobesedno. Potrebno je vzeti nekaj, kar je kongruentno $-1 \pmod{p}$. Tako število je npr. $p-1$. Vstavimo torej $b = p-1$ v začetno enačbo: $a+p-1 \mid f(a)+f(p-1)$. Sedaj vzamemo k, da je $a^k \equiv 1 \pmod{p}$ (npr. $k = p-1$). Sledi $p \mid a^k + p - 1$, torej $p \mid f(a)^k + f(p-1)$. Ampak za $f(p-1)$ vemo, da $p-1+1 \mid f(p-1)+1$, torej $p \mid f(p-1)+1$. S tem dobimo $p \mid f(a)^k - 1$, torej $f(a)^k \equiv 1 \pmod{p}$. Izsledek: če p ne deli a, potem $f(a)$ tudi ni deljivo s p. Poleg tega pa je $a \mid f(a)$, torej so prafaktorji $f(a)$ natanko tisti, ki so tudi prafaktorji a.

To je najmočnejše pri praštevilih: če vzamemo $a = p$, potem je $f(p)$ potenca p. Ker je funkcija multiplikativna, pa nas ravno te vrednosti zanimajo! Hura. Zdaj poskusimo ugotoviti, kakšne so te potence. Iz $p+1 \mid f(p)+1$ sledi $p+1 \mid p^k+1$, kjer je $f(p) = p^k$. To pa je možno natanko tedaj, ko je k lih. Zdaj pa predpostavimo, da $f(p) = p^k$ in $f(q) = q^l$ za različni praštevili p, q, in poskusimo dobiti $k = l$. Iz $a = p, b = q$ direktno ne dobimo ničesar.

Spet moramo uporabiti podoben trik kot na začetku. Če namesto q vstavimo q^t, imamo na voljo mnogo več pogojev. Iz $a = p, b = q^t$ sledi $p+q^t \mid f(p)+f(q^t) = p^k+q^{tl}$. Ampak $p+q^t \mid p^l+q^{tl}$, zato $p+q^t \mid p^k-p^l$. Sedaj za dovolj velike t dobimo $p^k - p^l = 0$, torej $k = l$. S tem smo ugotovili, da je $f(p) = p^k$ za nek lihi k, ki je enak za vsako praštevilo p. To po multiplikativnosti pomeni, da so edine rešitve $f(x) \equiv x^k$ za nek lih k. □

Naloga 2.7

Določi vse funkcije $f\colon \mathbb{N} \to \mathbb{N}$, da je $(f(m)+n)(f(n)+m)$ popoln kvadrat za vse $m, n \in \mathbb{N}$.

Dokaz. Poleg rešitve $f(n) = n$ delujejo še $f(n) = n + c$ za katerikoli nenegativni celi c. V takih situacijah je pogosto ideja, da od funkcije odštejemo neko konstanto in s tem zastonj dobimo dodatni pogoj. Tukaj to žal ne deluje, ker enačba postane neobvladljivo grda. Iz tega lahko sklepamo, da bo edini možen pristop ta, da namesto določanja samih vrednosti funkcije poskušamo najti kakšno relacijo med njimi.

Za nek fiksen n, m in $f(m)$ je možnih $f(n)$ ogromno. Po velikosti jih ne moremo omejiti, edina možnost je, da poskusimo forsirati kakšno deljivost. Opazimo, da če je en faktor deljiv z liho potenco praštevila p, bo tudi drugi, saj je njun produkt popoln kvadrat. Torej če vzamemo n tako, da je $\nu_p(f(m)+n)$ lih, bo tudi $\nu_p(f(n)+m)$ lih, torej $p \mid f(n)+m$. Bolj eksplicitno: če $n = kp - f(m)$ za sod $\nu_p(k)$, potem $f(kp - f(m)) \equiv -m \pmod{p}$.

A kaj s tem? Za poljuben m smo našli veliko možnih k, za katere $f(kp-f(m)) \equiv -m \pmod p$. Ideja je, da podobno naredimo še za drugo število m', kar nam da $f(k'p - f(m')) \equiv -m' \pmod p$ za sod $\nu_p(k')$. Ker imamo za k in k' veliko izbire, bi lahko našli takšna k in k', da je $kp-f(m) = k'p-f(m')$. S tem se znebimo grdega člena nad katerim nimamo nobene kontrole: ostane nam $m \equiv -f(kp - f(m)) \equiv -f(k'p - f(m')) \equiv m' \pmod p$. Seveda lahko taka k in k' obstajata samo, če je $f(m) - f(m')$ deljivo s p. Pa vendar se zdi, da je ta pogoj tudi zadosten, ker je k in k' s sodim ν_p veliko. To lahko dokažemo z malo truda in caseworka (pri $p = 2$ je malo več dela kot drugod, a se vseeno izide).

Sedaj smo končno ugotovili nekaj lepega: $p \mid f(m) - f(m') \implies p \mid m - m'$. To lahko najbolje izrabimo v primeru, da ima $m - m'$ malo prafaktorjev. Najboljši je $m - m' = 1$, kar nam da $f(m + 1) - f(m) = \pm 1$. Ta "diskretna zveznost" je zelo močna, saj lahko sedaj z indukcijo pokažemo, da je $f(n) = n + c$ za neko konstanto c in vse n. Začnemo pri $f(1)$ in vidimo $f(2) = f(1) \pm 1$, nato $f(3) = f(2) \pm 1$ itd. Predznak je enak za vse korake, saj drugače funkcija ne bi bila injektivna, kar bi bilo v protislovju s $p \mid f(m) - f(m') \implies p \mid m - m'$. Sledi $f(n) = c \pm n$, a ker so vrednosti funkcije naravna števila, je edina možnost $f(n) = n + c$ za neko nenegativno celo število c. □

3 Indukcijske

Naloga 3.1

Določi vse $f\colon \mathbb{N} \to \mathbb{N}$, za katere velja $f(a) + f(b) \mid 2(a + b - 1)$ za vse $a, b \in \mathbb{N}$.

Dokaz. Neumnosti: $a = b = 1$ da $2f(1) \mid 2$, torej je $f(1) = 1$. Nato $f(2) + 1 \mid 4$, torej $f(2) \in \{1, 3\}$. V prvem primeru po preprosti indukciji (vstavljanje $(a, 1)$, $(a, 2)$) sledi rezultat, saj dobimo $f(a) + 1 \mid 2a, 2a + 2 \implies f(a) + 1 \mid 2 \implies f(a) = 1$. V drugem pa se moramo malo bolj potruditi. Poglejmo si še $f(3)$ in $f(4)$. Iz $f(4) + 1 \mid 8$ ter $f(4) + 3 \mid 10$ sledi $f(4) = 7$, zato $f(3) + 7 \mid 12$ in $f(3) = 5$. Kaže, da bo v tem primeru rešitev $f(n) = 2n - 1$.

Za vse višje a uporabimo indukcijo. Denimo, da je $a > 4$ in $f(b) = 2b - 1$ za vse $b < a$. Tedaj sledi $f(a) + 2b - 1 \mid 2(a + b - 1) = 2a - 1 + 2b - 1$, zato $f(a) + 2b - 1 \mid 2a - 1 - f(a)$. Iz $b = 1$ sledi $f(a) + 1 \mid 2a$, torej $f(a) \leq 2a - 1$. Denimo, da $f(a) < 2a - 1$. Za $b = a - 1$ potem velja $f(a) + 2a - 3 \mid 2a - 1 - f(a)$, torej $f(a) + 2a - 3 \leq 2a - 1 - f(a)$, kar pomeni, da $f(a) = 1$. Potem iz $b = a - 2$ sledi še $1 + 2a - 5 \mid 2a - 2$, zato $2a - 4 \mid 2$, kar je nemogoče za $a > 4$. Sledi, da je $f(a) = 2a - 1$. □

Naloga 3.2

Določi vse funkcije $f\colon \mathbb{Z} \to \mathbb{Z}$, da za vse $a, b, c \in \mathbb{Z}$ z $a+b+c = 0$ velja $f(a)^2+f(b)^2+f(c)^2 = 2(f(a)f(b) + f(b)f(c) + f(c)f(a))$.

Dokaz. Neumnosti: $f(0) = 0$ in $f(-x) = f(x)$. Nato vstavimo $c = -a - b$: $f(a + b)^2 + f(a)^2 + f(b)^2 = 2(f(a)f(b) + (f(a) + f(b))f(a + b))$. Torej $f(a + b)^2 - 2(f(a) + f(b))f(a + b) + (f(a) - f(b))^2 = 0$.

Rešimo za $f(a + b)$, kar nam da $f(a + b) = f(a) + f(b) \pm \sqrt{((f(a) + f(b))^2 - (f(a) - f(b))^2)} = f(a) + f(b) \pm 2\sqrt{f(a)f(b)}$. Zdaj je smiselno vzeti $a = b = 1$, kar da $f(2) = 2f(1) \pm 2\sqrt{f(1)^2}$.

Torej je ali $f(2) = 4f(1)$ ali $f(2) = 0$. Drugi primer vodi do 0 na sodih, $f(1)$ na lihih, kar deluje.

V prvem primeru pa $f(3) = 5f(1) \pm 4f(1)$, torej ali $f(3) = 9f(1)$ ali $f(3) = f(1)$. Prvi vodi do $f(n) = n^2 f(1)$ (prištevamo po 1 in 2), drugi pa do $f(1)$ na lihih, 0 na deljivih s 4, in $4f(1)$ na ostalih sodih. □

Naloga 3.3

Določi vse $f\colon \mathbb{N} \to \mathbb{N}$, za katere za vse $a, b \in \mathbb{N}$ obstaja nedegeneriran trikotnik s stranicami dolžin a, $f(b)$ in $f(b + f(a) - 1)$.

Dokaz. Splača se $a = 1$, dobimo $f(b) = f(b + f(1) - 1)$, torej je f ali periodična, ali pa $f(1) = 1$. Če je periodična, je omejena, kar ne gre (vstavi dovolj veliki a). Torej je $f(1) = 1$. Sedaj vstavimo $b = 1$, kar da $a = f(f(a))$. Posebej je f bijekcija. Splačalo se je $a = 1$, morda se splačajo še drugi majhni a, npr. 2. Dobimo $|f(b + f(2) - 1) - f(b)| < 2$, torej se spremeni kvečjemu za 1 ($f(2) \neq 1$). Za 0 ne gre po injektivnosti. Če začnemo z $b = 1$, dobimo $f(1 + f(2) - 1) = 2$, nato $f(1 + 2(f(2) - 1)) = 3$ itd. po injektivnosti. Sledi, da na tem aritmetičnem zaporedju funkcija doseže vsa naravna števila, torej je to zaporedje ves $\mathbb{N}$ in $f(x) = x$. □

Naloga 3.4

Najdi vse $f\colon \mathbb{N} \to \mathbb{N}$, za katere za vsaka $a, b \in \mathbb{N}$ velja $f(ab) = f(a)f(b)$ in sta vsaj dve izmed števil $f(a), f(b)$ in $f(a + b)$ enaki.

Dokaz. Najprej poskusimo uganiti množico rešitev. Kdor se spozna na teorijo števil, verjetno vidi podobnost med 2. pogojem naloge in lastnostjo funkcije ν_p. Da bi ustregli še 1. pogoju pa raje uporabimo $f(n) = c^{\nu_p(n)}$ za nek $c \in \mathbb{N}$ in $p \in \mathbb{P}$. Nekako želimo priti do teh števil; najbolj smiseln način je, da vzamemo najmanjše število, za katerega je $f(n) > 1$. Ta n mora biti praštevilo, saj bi sicer $n = ab$ za $a, b > 1$, iz česar bi sledilo $f(a)f(b) > 1$, torej n ne bi bil minimalen. Pišimo torej p namesto n in c namesto $f(p)$.

Sedaj poglejmo, katere vrednosti f lahko iz tega izračunamo. Za začetek, $f(p^2) = c^2$ in $f(kp) = c$ za $k < p$. Ali lahko pridobimo še ostala števila v $[p, p^2]$, ki so tuja p? Za začetek si poglejmo števila v $[p^2 - p + 1, p^2 - 1]$: iz 2. pogoja (za $(a, b) = (p^2 - k, k)$ in $k < p$) sledi, da sta med $f(p^2 - k)$, $f(k)$ in $f(p^2)$ vsaj dve števili enaki. To pomeni, da $f(p^2 - k) \in \{1, c^2\}$. Poleg tega iz $(a, b) = (p^2 - p, p - k)$ sledi $f(p^2 - k) \in \{1, c\}$. Torej $f(p^2 - k) = 1$. Naš cilj je ta postopek posplošiti še na ostala števila $n \in [p, p^2]$, tuja p, tj. povezati vrednost $f(n)$ najprej s $f(p^2) = c^2$ in nato še z nekim $f(kp) = c$. Tako bi spet dobili $f(n) \in \{1, c^2\}$ in $f(n) \in \{1, c\}$.

Žal nam istega postopka ne uspe izvesti: za $n = qp + r$ ($1 \leq q, r < p$) iz $(a, b) = (qp, r)$ dobimo $f(n) \in \{1, c\}$, s $f(p^2)$ pa nam $f(n)$ ne uspe direktno povezati na enak način kot prej. "Trik" je v tem, da obrnemo vlogi n in p: raje zapišimo $p^2 = qn + r$ za $1 \leq q \leq \frac{p^2}{n} < p, 0 \leq r < n$. Velja še $p \nmid r$, saj bi sicer $p \mid qn$, kar ni mogoče. Sledi $f(r) = 1$, če delamo indukcijo po n! Pa jo delajmo. Dobimo torej, da sta vsaj dve od $f(qn) = f(q)f(n) = f(n), f(r) = 1$ in $f(p^2) = c^2$ enaki, oziroma, končno, $f(n) \in \{1, c^2\}$. To zaključi indukcijski korak!

Podobna strategija deluje tudi za števila nad p^2. Če je n deljiv s p, je vrednost $f(n)$ na

dlani (zaradi multiplikativnosti). Če pa ni, vzemimo prvo potenco p, ki je večja od n, in pišimo $p^k = qn + r$ za $1 \leq q \leq \frac{p^k}{n} < p, 0 \leq r < n$. Spet velja $p \nmid r$, zato $f(r) = 1$, in pa $f(qn) = f(n)$. Tako dobimo $f(n) \in \{1, c^k\}$. Podobno za $n = tp + s$, $1 \leq s < p$, dobimo $f(n) \in \{f(tp), f(s)\} = \{c^x, 1\}$ za nek $x \geq 1$. S tem dobimo $f(n) = 1$ in zaključimo indukcijo ter dokaz. □

Naloga 3.5

Določi vse funkcije $f\colon \mathbb{N} \to \mathbb{N}$, za katere velja $d(f(x)) = d(x)$ za vse $x \in \mathbb{N}$ in $\gcd(f(x), f(y)) > f(\gcd(x, y))$ za vse $x, y \in \mathbb{N}$, ki zadoščajo $x \nmid y$ in $y \nmid x$.

Dokaz. Za začetek opazimo, da je $f(1) = 1$, saj je to edino število z enim deliteljem. Podobno za vsa praštevila p velja, da je $f(p)$ praštevilo. Če sta p in q različni, potem $\gcd(f(p), f(q)) > f(\gcd(p, q)) = f(1) = 1$, kar pomeni, da je $f(p) = f(q)$, torej je f na praštevilih konstantno enaka nekemu praštevilu c.

Ideja bo indukcija po številu deliteljev. Naj bo $n = \prod_{i=1}^{k} p_i^{a_i}$ število s $k \geq 3$ delitelji. Predpostavimo, da za vsa števila z manj kot k delitelji velja $f(m) = c^{d(m)-1}$. Da določimo $f(n)$, izberemo $x = n$ in y tak, da je $y \nmid n$ in $n \nmid y$, ter da ima y manj kot k deliteljev. Hkrati pa si želimo, da ima $\gcd(n, y)$ čim več deliteljev. Možnost je npr. $y = n \cdot \frac{q}{p}$ za dve različni praštevili p, q. Da to deluje, mora seveda veljati $p \mid n$. Število deliteljev y je potem $d(n) \cdot \frac{\nu_p(n)}{\nu_p(n)+1} \cdot \frac{\nu_q(n)+2}{\nu_q(n)+1}$, kar je manj kot $d(n)$, če $\frac{\nu_p(n)}{\nu_p(n)+1} \cdot \frac{\nu_q(n)+2}{\nu_q(n)+1} < 1$. To je ekvivalentno $\frac{\nu_p(n)}{\nu_p(n)+1} < \frac{\nu_q(n)+1}{\nu_q(n)+2} \iff 1 - \frac{1}{\nu_p(n)+1} < 1 - \frac{1}{\nu_q(n)+2} \iff \frac{1}{\nu_q(n)+2} < \frac{1}{\nu_p(n)+1} \iff \nu_p(n) + 1 < \nu_q(n) + 2$, kar velja če in samo če $\nu_p(n) \leq \nu_q(n)$. Torej bo potrebno tudi $q \mid n$; za potence praštevil bomo morali poskrbeti kasneje. Kaj smo dobili s to izbiro y?

$$\gcd(f(n), c^{d\left(\frac{nq}{p}\right)-1}) = \gcd(f(n), f(y)) > f(\gcd(n, y)) = f(\frac{n}{p}) = c^{d\left(\frac{n}{p}\right)-1},$$

oziroma $c^{d\left(\frac{n}{p}\right)} \mid f(n)$. In ker $d\left(\frac{n}{p}\right) \geq \frac{k}{2}$, sledi $c^{\lfloor \frac{k}{2} \rfloor} \mid f(n)$. Če bi $f(n)$ imel še kak prafaktor, različen od c, bi bilo $d(f(n)) \geq 2(\lfloor \frac{k}{2} \rfloor + 1)$, a to je strogo več od $k = d(n)$: protislovje. Sledi, da $f(n) = c^{k-1}$.

Preostal nam je še primer, ko je $n = p^{k-1}$ za neko praštevilo p. Tu uporabimo podoben trik, le da vzamemo $y = p^{\lfloor \frac{k}{2} \rfloor - 1} q$, kjer je q praštevilo, različno od p. Tu dobimo $d(y) = 2\lfloor \frac{k}{2} \rfloor \leq k$. Za ta y poznamo $f(y)$: če $k = d(y)$, je k sod, zato ≥ 4 in ima y vsaj dva različna prafaktorja, torej smo zanj poskrbeli že v prejšnjem odstavku. Sledi

$$\gcd(f(n), c^{2\lfloor \frac{k}{2} \rfloor - 1}) = \gcd(f(n), f(y)) > f(\gcd(n, y)) = f(p^{\lfloor \frac{k}{2} \rfloor - 1}) = c^{d(p^{\lfloor \frac{k}{2} \rfloor - 1})-1} = c^{\lfloor \frac{k}{2} \rfloor - 1},$$

torej $c^{\lfloor \frac{k}{2} \rfloor} \mid f(n)$. Kot prej, če bi imel $f(n)$ še kak drug prafaktor, bi dobili protislovje, saj bi njegovo število deliteljev preseglo k. Sledi $f(n) = c^{k-1}$ tudi v tem primeru, kar zaključi indukcijski korak in s tem dokaz. □

4 Posladek: konstrukcijske

Naloga 4.1

Ali obstaja funkcija $f\colon \mathbb{N} \to \mathbb{N}$, da za vse $n \in \mathbb{N}$ velja $f(f(n)) = 2n$?

Dokaz. Poskusimo zgraditi tako funkcijo. Za začetek uporabimo klasičen trik pri takih "involucijskih" enačbah: vstavimo $f(n)$. To nam da $f(f(f(n))) = 2f(n)$. Po začetni enačbi pa je $f(f(f(n))) = f(2n)$, torej $f(2n) = 2f(n)$ za vse n.

Oglejmo si zaporedje, ki ga dobimo z zaporedno uporabo funkcije na številu 1:

$$1, f(1), f(f(1)) = 2, f(2) = 2f(1), f(f(2)) = 4, f(4) = 2f(2) = 4f(1), f(f(4)) = 8, \ldots$$

Členi na sodih mestih so oblike 2^k, ostali pa $2^k f(1)$. Funkcijska enačba je s tem zadovoljena za vsa števila v tej verigi, za poljubno izbiro $f(1)$.

Seveda število 1 pri tem ni igralo ključne vloge. Tako lahko podobno naredimo za poljubno število m, ki še ni v nobeni verigi, ki smo jo že naredili. Tako lahko poskusimo pokriti vsa naravna števila. Eksplicitna izbira je lahko npr $f(1) = 3$, $f(5) = 7$, itd. (verige začnemo z novim lihim številom, drugi člen pa je naslednje prosto liho število), kar očitno deluje. □

Naloga 4.2

Ali obstaja bijekcija $f\colon \{1 + 3n \mid n \in \mathbb{N}_0\} \to \{1 + 4n \mid n \in \mathbb{N}_0\}$, za katero velja $f(xy) = f(x)f(y)$ za vse $x, y \in \{1 + 3n \mid n \in \mathbb{N}_0\}$?

Dokaz. Ideja je, da se fokusiramo na praštevila, saj so multiplikativne funkcije (vsaj konceptualno) določene s svojimi vrednostmi na praštevilih. Težava je, da imajo števila oblike $3n + 1$ tudi prafaktorje oblike $3n + 2$, ki sploh niso v domeni naše funkcije. Kaj storiti z njimi? Če jih ne bi bilo, bi lahko preprosto preslikali vsako praštevilo oblike $3n + 1$ v praštevilo oblike $4n + 1$ in zaključili.

Ključ je, da za vsako praštevilo oblike $3n + 2$ najdemo praštevilo oblike $4n + 3$ in ga uporabimo kot "sliko", četudi tega praštevila ni v kodomeni, ampak se pojavi le v faktorizaciji števil v naši množici. Tako lahko (po Dirichletovem izreku) najdemo bijekciji med praštevili oblike $3n + 1$ in $4n + 1$ ter med praštevili oblike $3n + 2$ in $4n + 3$. Zdaj pa lahko definiramo funkcijo na vseh številih oblike $3n + 1$ tako, da faktoriziramo število na praštevila, nato pa vsako preslikamo s prej določenima bijekcijama in zmnožimo rezultate. To deluje. (V ozadju je ključno dejstvo, da sta grupi $(\mathbb{Z}/3\mathbb{Z})^\times$ in $(\mathbb{Z}/4\mathbb{Z})^\times$ izomorfni.) □