Seriál – Teorie čísel III

A je tu třetí, závěrečný, opět o něco kratší díl seriálu! K jeho přečtení nebudeš příliš potřebovat látku předchozích dílů, spíš bude nutné nebát se a pořádně se zamýšlet. Odměnou Ti bude kus krásné matematiky, který sice tolik nevyužiješ v olympiádě, ale pro který stojí za to žít.

Na co se tedy můžeš těšit? Nejprve se naučíš zkrotit hrůzostrašně vyhlížející sumy. Poté se seznámíš s všelijakými aritmetickými funkcemi, naučíš se je chytře násobit a vše využiješ k jednoduchým a extrémně elegantním důkazům překvapivých identit.

Práce se sumami

V tomto díle budeme často používat složitější úpravy výrazů se sumami. Jedná se sice o techničtější část matematiky, ale zjistíš, že se v ní ukrývají i pěkné triky. Práci se sumami navíc mnohokrát zúročíš i v dalších oborech. Nejprve si zopakujeme sumární zápis a poté si ukážeme základní úpravy, které nám později ulehčí život.

Symbol $\sum$ značí součet několika členů, a to v různých kontextech, jak se nejlépe ukáže na příkladech. Mějme nějakou funkci f.

(i) Definujeme $\sum_{k=1}^{n} f(k) = f(1) + f(2) + \cdots + f(n)$. Suma tedy vyjadřuje následující: Nejprve za k dosaďme 1, potom 2, 3, … a nakonec n. Všechny tyto členy sečtěme. Například

$$\sum_{k=1}^{n} 1 = n, \quad \sum_{m=2}^{4} (m^2+1) = 32 = 1 + \sum_{n=0}^{4} 2^n.$$

(ii) Výraz $\sum_{d|n} f(d)$ vyjadřuje součet $f(d)$ přes všechny kladné dělitele d čísla n. Tedy

$$\sum_{d|18} d^2 - 1 = (1^2-1) + (2^2-1) + (3^2-1) + (6^2-1) + (9^2-1) + (18^2-1).$$

(iii) Obecně $\sum_{i \in I} f(i)$ znamená součet přes všechny prvky množiny I. Třeba

$$\sum_{i \in \{1,\,3,\,-6,\,8\}} f(i) = f(1) + f(3) + f(-6) + f(8).$$

(iv) Také se nám může stát, že potřebujeme sčítat přes dvě proměnné. Například

$$\sum_{2 \le a,b \le 3} f(a) \cdot f(b) = f(2)^2 + f(2)f(3) + f(3)f(2) + f(3)^2,$$

$$\sum_{\substack{2 \le i \le 4 \\ d \,|\, i}} \frac{f(i)}{f(d)} = \frac{f(2)}{f(1)} + \frac{f(2)}{f(2)} + \frac{f(3)}{f(1)} + \frac{f(3)}{f(3)} + \frac{f(4)}{f(1)} + \frac{f(4)}{f(2)} + \frac{f(4)}{f(4)}.$$

Proměnnou k (resp. d, m, n, i, a, b), přes kterou jsme v sumě sčítali, nazýváme index a automaticky ji považujeme za celé číslo. Ukažme ještě jeden konkrétní příklad s vnořenými sumami:

$$\sum_{d|4}\sum_{a=1}^{d} 2a = (2) + (2+4) + (2+4+6+8) = 28.$$

Vytknutí čísla před sumu

První často používanou úpravou je vytknutí čísla před sumu. Když máme uvnitř sumy součin a jeden z činitelů je nezávislý na sčítacím indexu, můžeme tento činitel vytknout před sumu. Jedná se o běžné vytknutí, jak ho známe, jen u sum může působit nezvykle. Například

$$\begin{aligned}\sum_{i=1}^{n} n\cdot(n+i-1) &= n\cdot n + n\cdot(n+1) + \cdots + n\cdot(2n-1)\\ &= n\cdot\big(n + (n+1) + \cdots + (2n-1)\big)\\ &= n\cdot\sum_{i=1}^{n}(n+i-1).\end{aligned}$$

Prohazování sum

Často se nám stane, že máme dvě sumy vedle sebe. Pak je můžeme prohodit. Například

$$\sum_{i=1}^{n}\sum_{j=1}^{m} f(i)\cdot g(j) = \sum_{j=1}^{m}\sum_{i=1}^{n} f(i)\cdot g(j).$$

Uvědomme si, že se opravdu nic nezměnilo. Když si totiž představíme čísla $f(i)\cdot g(j)$ v tabulce s m řádky a n sloupci, tak levá strana vyjadřuje, že jsme udělali součty v každém ze sloupců a výsledky jsme pak sečetli. Naproti tomu na pravé straně jsme sečetli součty řádků. Zřejmě jsme tedy dostali v obou případech stejné číslo – součet všech čísel v tabulce. Na ten se taky můžeme dívat jako na sumu

$$\sum_{\substack{1\le i\le n\\ 1\le j\le m}} f(i)\cdot g(j).$$

Prohazování sum se dá vhodně kombinovat s vytýkáním:

$$\sum_{i=1}^{n}\Big(f(i)\sum_{j=1}^{m} g(j)\Big) = \sum_{i=1}^{n}\sum_{j=1}^{m} f(i)\cdot g(j) = \sum_{j=1}^{m}\sum_{i=1}^{n} f(i)\cdot g(j) = \sum_{j=1}^{m}\Big(g(j)\sum_{i=1}^{n} f(i)\Big).$$

To se může hodit například, pokud neumíme vyjádřit součet $\sum_{i=1}^{m} g(i)$, ale součet $\sum_{i=1}^{n} f(i)$ ano. První, resp. poslední výraz v předchozí rovnosti se dá taky upravit dalším vytknutím na součin dvou sum, tedy na

$$\Big(\sum_{i=1}^{n} f(i)\Big)\cdot\Big(\sum_{j=1}^{m} g(j)\Big).$$

Prohození sum je ještě o trochu komplikovanější, když prvky, přes které sčítáme ve vnitřní sumě, jsou závislé na indexu vnější sumy. Například $\sum_{d|n}\sum_{e|d} f(e)$. Chtěli bychom na první místo dostat sumu přes e. K tomu si stačí uvědomit, že e je dělitel čísla n. Tedy vnější suma

bude $\sum_{e|n}$. A jaké nyní klást podmínky na d? Musí platit, že d je násobek e a přitom $d \mid n$. Vnitřní suma proto bude $\sum_{\substack{d=e\cdot x \\ d\mid n}}$. Výraz tak upravíme do podoby

$$\sum_{d|n}\sum_{e|d} f(e) = \sum_{e|n}\sum_{\substack{d=e\cdot x \\ d\mid n}} f(e) = \sum_{e|n}\Big(f(e)\sum_{\substack{d=e\cdot x \\ d\mid n}} 1\Big).$$

Rozmysli si, že jsme opravdu žádný člen nevypustili a žádný nezapočítali vícekrát.

Cvičení. Opravdu si to rozmysli.

Nyní uvidíme, proč se prohození sum vyplatilo. Vnitřní sumu totiž umíme dál pěkně upravit. Sčítáme několikrát jedničku, stačí jen zjistit kolikrát. Jinak řečeno, vnitřní suma se rovná počtu takových čísel d, že $d = ex$ a zároveň $d \mid n$. Tedy $ex \mid n$, a jelikož $e \mid n$, tak $x \mid \frac{n}{e}$. Počet vyhovujících čísel d je proto stejný jako počet x takových, že $x \mid \frac{n}{e}$. Odpovědí je tedy počet dělitelů čísla $\frac{n}{e}$. Pokud označíme $\tau(n)$ počet dělitelů čísla n, tak jsme původní výraz upravili na

$$\sum_{d|n}\sum_{e|d} f(e) = \sum_{e|n} f(e)\cdot\tau\Big(\frac{n}{e}\Big). \qquad (\heartsuit)$$

Aritmetické funkce

V této kapitole se dostáváme k hlavnímu programu našeho seriálu – aritmetickým funkcím. Budeme je zkoumat, sčítat, násobit (a možná jinak, než bys čekal(a)), a díky tomu si odvodíme mnoho zajímavých výsledků teorie čísel. Co to tedy je?

Definice. *Aritmetická funkce* je funkce z přirozených čísel do reálných čísel.[6]

Příkladem aritmetických funkcí jsou funkce $f(n) = n^3$, $f(n) = \log(n)$ nebo Eulerova funkce $\varphi(n)$.

Zajímavé aritmetické funkce dostaneme, když vezmeme všelijaké vlastnosti čísla n týkající se dělitelnosti.

Definice. Aritmetickou funkcí $\tau(n)$ myslíme počet všech kladných dělitelů čísla n.[7] Součet všech kladných dělitelů čísla n označujeme jako $\sigma(n)$.

S těmito aritmetickými funkcemi jsme se vlastně již setkali – zmiňovali jsme totiž dokonalá čísla, což jsou přesně ta čísla n, pro která platí $\sigma(n) = 2n$.

Počet dělitelů $\tau(n)$ můžeme snadno vyjádřit, pokud známe rozklad čísla n na prvočísla.

Tvrzení. *Nechť $n = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ je rozklad čísla n na prvočísla. Pak platí*

$$\tau(n) = (\alpha_1+1)\cdots(\alpha_r+1).$$

Důkaz. Stačí si uvědomit, že každý dělitel obsahuje ve svém rozkladu pouze prvočísla $p_1, \ldots, p_r$, přičemž prvočíslo p_i v mocnině 0 až α_i. To je tedy $(\alpha_i + 1)$ možností pro prvočíslo p_i. Jelikož můžeme exponenty u různých prvočísel volit nezávisle na sobě, zjistíme počet všech dělitelů jako součin těchto výrazů.

[6] Nebo dokonce komplexních. Aritmetické funkce jsou vlastně jen jiný pohled na posloupnosti.

[7] Mluvíme o ní krátce jako o *počtu dělitelů*.

Podobný vzorec závislý na rozkladu na prvočísla existuje i pro součet dělitelů. K němu přirozeně dospějeme v kapitole o multiplikativních funkcích, zatím si jen uvědomíme, že platí následující.

Tvrzení. *Pro součet dělitelů mocniny prvočísla platí* $\sigma(p^k) = \frac{p^{k+1}-1}{p-1}$.

Důkaz. Jedná se pouze o známý[8] vztah pro součet geometrické řady $1+p+\cdots+p^k$. Se znalostí tohoto vzorečku už snadno požadovaný výsledek dokážeš.

Seznámíme se nyní s další aritmetickou funkcí – Möbiovou funkcí μ, která hraje v následující teorii klíčovou roli.

Definice. *Möbiova*[9] *funkce* μ je

$$\mu(n) = \begin{cases} 1 & \text{pro } n = 1, \\ 0, & \text{je-li } n \text{ čtvercové, tedy existuje-li } a > 1 \text{ takové, že } a^2 \mid n, \\ (-1)^r, & \text{je-li } n = p_1 p_2 \cdots p_r, \text{ kde } p_i \text{ jsou navzájem různá prvočísla.} \end{cases}$$

Například $\mu(4) = 0$, $\mu(5) = -1$, $\mu(6) = 1$. Jednu z pěkných vlastností Möbiovy funkce ukazuje následující důležité tvrzení.

Tvrzení. *Platí:*

$$\sum_{d|n} \mu(d) = \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1 & \text{pro } n = 1, \\ 0 & \text{pro } n > 1. \end{cases} \qquad (\clubsuit)$$

Důkaz. Všimněme si, že pokud jsou a, b nesoudělná, platí $\mu(a)\mu(b) = \mu(ab)$. Pro $n = 1$ je triviálně součet roven jedné. Máme-li $n > 1$, můžeme ho rozložit na prvočísla, $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Jediní dělitelé čísla n, kteří do sumy přispějí, jsou ti bezčtvercoví. Proto můžeme psát (vyzkoušej si, že po roznásobení prostředního výrazu opravdu dostaneme každé nenulové číslo ze součtu nalevo právě jednou)

$$\sum_{d|n} \mu(d) = (1 + \mu(p_1))(1 + \mu(p_2)) \ldots (1 + \mu(p_r)) = 0 \cdot 0 \cdots 0 = 0,$$

což jsme chtěli dokázat.

Dirichletova konvoluce

Nyní již umíme sčítat sumy a můžeme se vrhnout na tento příklad (dobře si ho promysli).

Příklad. Ukaž, že pro $n \geq 1$ platí

$$\varphi(n) = \sum_{d|n} \mu(d) \cdot \frac{n}{d}.$$

Řešení. Nejprve si uvědomíme, že výraz $\lfloor 1/(a,b) \rfloor$ je roven jedné, právě když jsou čísla a, b nesoudělná, jinak je to nula. Proto se $\varphi(n)$ dá vyjádřit jako tato suma:

$$\varphi(n) = \sum_{k=1}^{n} \left\lfloor \frac{1}{(n,k)} \right\rfloor.$$

[8] A snadno vygooglitelný.

[9] August Ferdinand Möbius (1790–1868) byl německý matematik a teoretický astronom. Kromě toho, že se věnoval teorii čísel, byl také jedním ze zakladatelů topologie. Pravděpodobně jsi už slyšel(a) o Möbiově pásce.

Následně využijeme vztahu (♣) pro každý ze sčítanců sumy a dostaneme

$$\varphi(n) = \sum_{k=1}^{n} \left\lfloor \frac{1}{(n,k)} \right\rfloor = \sum_{k=1}^{n} \sum_{d\mid(n,k)} \mu(d) = \sum_{k=1}^{n} \sum_{\substack{d\mid n\\ d\mid k}} \mu(d).$$

Nyní přichází čas na prohození sum, které je opět poměrně náročné, pročež si jej dobře rozmysli.

$$\sum_{k=1}^{n} \sum_{\substack{d\mid n\\ d\mid k}} \mu(d) = \sum_{d\mid n} \sum_{\substack{k=dx\\ k\le n}} \mu(d) = \sum_{d\mid n} \Big(\mu(d) \sum_{\substack{k=dx\\ k\le n}} 1\Big).$$

Zbývá si uvědomit, že poslední vnitřní suma vyjadřuje jen počet násobků čísla d menších nebo rovných n. A jelikož $d \mid n$, je jich přesně $\frac{n}{d}$. Tím jsme dostali požadovaný vztah, který si připomeneme pro případ, že už jsi zapomněl(a), co vlastně dokazujeme:

$$\varphi(n) = \sum_{d\mid n} \mu(d) \cdot \frac{n}{d}.$$

Poznámka. Součet v minulém příkladu je speciálním případem výrazu

$$\sum_{d\mid n} f(d) \cdot g\Big(\frac{n}{d}\Big),$$

kde f a g jsou aritmetické funkce. Takovéto součty se v teorii čísel často objevují a my se nyní budeme zabývat jejich obecnými vlastnostmi.

Předtím si zavedeme ještě dvě jednoduché, ale užitečné aritmetické funkce:

Definice. *Jednotka* je aritmetická funkce u, která všem číslům přiřadí jedničku (tedy $u(n) = 1$ pro každé n.)[10]

Definice. Aritmetická funkce N je definovaná vztahem $N(n) = n$ pro každé n.[11]

Definice. *Dirichletova konvoluce*[12] aritmetických funkcí f a g je aritmetická funkce

$$h(n) = \sum_{d\mid n} f(d) \cdot g\Big(\frac{n}{d}\Big).$$

Konvoluci funkcí f a g značíme $f * g$.

Konvoluce je tedy operace, která vezme dvě aritmetické funkce a vyrobí z nich třetí. Na příkladu jsme viděli, že když zvolíme za f Möbiovu funkci μ a za g funkci N, dostaneme φ, jinými slovy $\varphi = \mu * N$.

Jiným zajímavým příkladem jsme zakončili první díl seriálu, když jsme si ukázali, že platí

$$n = \sum_{d\mid n} \varphi(d).$$

Tento vztah neříká nic jiného, než že $N = \varphi * u$. V takovémto případě, kdy je jedna z funkcí v konvoluci u, zavádíme nový pojem.

[10] Značení vychází z anglického slova *unit*.

[11] Značení vychází z českého slova *nuda*.

[12] Můžeš se také setkat s pojmem Dirichletův součin. My budeme v seriálu říkat jednoduše konvoluce.

Definice. Nechť f je aritmetická funkce. Pak aritmetickou funkci $g = f * u$, tedy $g(n) = \sum_{d|n} f(d)$, nazveme *sumární funkcí* funkce f.

Cvičení. Najdi sumární funkci k N.

Tvrzení. (Obecné vlastnosti konvoluce) *Nechť f, g, h jsou libovolné aritmetické funkce. Pak platí:*

(i) $f * g = g * f$, *(komutativita)*
(ii) $(f * g) * h = f * (g * h)$. *(asociativita)*

Říkáme, že je konvoluce komutativní a asociativní, což jinými slovy znamená, že nezáleží na tom, v jakém pořadí konvoluci provádíme, ani jak uzávorkujeme výrazy typu $f * g * h * i * j * k$.

Důkaz.

(i) K důkazu komutativity je třeba si uvědomit, že

$$\sum_{d|n} f(d)\, g\Big(\frac{n}{d}\Big) = \sum_{a\cdot b=n} f(a)\, g(b) = \sum_{b\cdot a=n} f(b)\, g(a) = \sum_{d|n} f\Big(\frac{n}{d}\Big)\, g(d),$$

kde prostřední sumy probíhají přes všechny dvojice čísel (a, b), pro které platí $ab = n$.

(ii) Označme $A = g * h$ a upravme $f * A = f * (g * h)$. Máme

$$\begin{aligned}(f * A)(n) &= \sum_{a\cdot d=n} f(a)\, A(d) = \sum_{a\cdot d=n} f(a) \sum_{b\cdot c=d} g(b)\, h(c)\\ &= \sum_{a\cdot b\cdot c=n} f(a)\, g(b)\, h(c).\end{aligned}$$

Je vidět, že pokud analogicky upravujeme výraz $((f*g)*h)(n)$, dospějeme ke stejnému výsledku.

Ještě se seznámíme s funkcí, která „nechává jiné funkce na pokoji“.[13]

Definice. *Identita* je aritmetická funkce I definovaná jako

$$I(n) = \Big\lfloor \frac{1}{n} \Big\rfloor = \begin{cases} 1 & \text{pro } n = 1,\\ 0 & \text{pro } n > 1.\end{cases}$$

Tvrzení. *Nechť f je aritmetická funkce. Pak platí $f * I = I * f = f$.*

Důkaz. Viz cvičení.

Cvičení. Tvrzení si dokaž.

Cvičení. Najdi sumární funkci k I.

Poznámka. V sekci o Möbiově funkci μ jsme si dokázali, že

$$\sum_{d|n} \mu(d) = \Big\lfloor \frac{1}{n} \Big\rfloor = I.$$

Pokud tento vztah přeložíme do řeči konvoluce, dostaneme, že $I = \mu * u$. Tento vztah částečně vysvětluje, proč je zrovna Möbiova funkce tak zajímavá. Je to totiž přesně ta funkce, jejíž sumární funkcí je I.

[13] Dokonce nechává na pokoji i sama sebe.

Nyní si můžeme ukázat, jaká síla se ukrývá v základních vlastnostech konvoluce.

Příklad. Dokážeme si novým a jednodušším způsobem, že

$$\varphi(n) = \sum_{d|n} \mu(d) \cdot \frac{n}{d},$$

neboli $\varphi = \mu * N$.

Důkaz. Z prvního dílu víme, že $N = \varphi * u$. To znamená, že také $N * \mu = (\varphi * u) * \mu$. Pravá strana se díky asociativitě(!) rovná $\varphi * (u * \mu)$. Navíc víme, že $u * \mu = I$, takže $N * \mu = \varphi * I = \varphi$. Jak snadné (a bez sum).

Poznámka. Vzpomeňme si nyní, kolik jsme museli udělat úprav, než jsme dostali vztah (♡) v kapitole o sumách:

$$\sum_{d|n} \sum_{e|d} f(e) = \sum_{e|n} f(e)\, \tau\left(\frac{n}{e}\right).$$

Přitom si stačí uvědomit, že výraz na levé straně je sumární funkce ze sumární funkce z f. Tedy $(f * u) * u$. S využitím asociativity víme, že se to rovná $f * (u * u)$, ale $u * u$ není nic jiného než $\sum_{d|n} 1$, tedy počet dělitelů $\tau(n)$ čísla n. Tedy $(f * u) * u = f * \tau$, což je výraz na pravé straně.

Řešení druhé čokoládové úlohy – náročnější pasáž

Jako příklad využití nabytých znalostí si ukážeme, jak se řešila druhá čokoládová úloha k minulé sérii, jejíž řešení nám bohužel nikdo neposlal.

Úloha. V závislosti na prvočísle p urči v $\mathbb{Z}_p$ součet všech primitivních prvků modulo p.

Řešení. Vezměme si nějaký primitivní prvek g modulo p (z minulého dílu víme, že existuje). Hledaný součet pak je

$$\sum_{\substack{1 \le k \le p-1 \\ (k,p-1)=1}} g^k,$$

což vyplývá z tvrzení zmíněného ve druhém díle, že g^k je primitivní prvek, právě když čísla k a $p-1$ jsou nesoudělná. V kapitole o aritmetických funkcích jsme si dokázali tvrzení

$$\sum_{d|n} \mu(d) = I(n).$$

Díky tomu lze naši sumu takto upravit:

$$\sum_{\substack{1 \le k \le p-1 \\ (k,p-1)=1}} g^k = \sum_{k=1}^{p-1} g^k \cdot I((k,p-1)) = \sum_{k=1}^{p-1} g^k \sum_{d|(k,p-1)} \mu(d) = \sum_{k=1}^{p-1} g^k \sum_{\substack{d|k \\ d|p-1}} \mu(d).$$

Podařilo se nám získat vnořené sumy, které můžeme prohodit, tak hurá do toho. Ve vnější sumě budeme tedy sčítat přes $d \mid p-1$ a ve vnitřní přes taková k, která jsou násobkem d a pro která platí $k \le p-1$. Pokud napíšeme $k = dr$, můžeme místo přes k sčítat přes r od 1 do $\frac{p-1}{d}$.

$$\sum_{k=1}^{p-1} g^k \sum_{\substack{d|k \\ d|p-1}} \mu(d) = \sum_{k=1}^{p-1} \sum_{\substack{d|k \\ d|p-1}} g^k \cdot \mu(d) = \sum_{d|p-1} \sum_{r=1}^{(p-1)/d} g^{rd} \cdot \mu(d) = \sum_{d|p-1} \mu(d) \sum_{r=1}^{(p-1)/d} g^{rd}.$$

Nyní stačí zjistit, čemu se rovná vnitřní suma. Pro $d = p-1$ je kongruentní s 1 modulo p. Pro $d \mid p-1$, $d < p-1$ stačí jen sumu sečíst jako geometrickou řadu, čímž dostaneme

$$\sum_{r=1}^{(p-1)/d} g^{rd} = g^d \frac{(g^d)^{(p-1)/d} - 1}{g^d - 1}.$$

Z Malé Fermatovy věty plyne $p \mid g^{p-1} - 1 = (g^d)^{(p-1)/d} - 1$, ale přitom $p \nmid g^d - 1$ (protože g je primitivní prvek a $d < p-1$). Tyto členy nám tudíž modulo p vypadnou a zůstane jen $\mu(p-1)$, což je řešení úlohy.

Multiplikativita funkcí

Většina aritmetických funkcí, se kterými jsme se dosud v seriálu setkali a se kterými se zde ještě setkáme, má významnou[14] vlastnost, které se říká multiplikativita.

Definice. O aritmetické funkci f řekneme, že je *multiplikativní*, pokud pro každou dvojici a, b přirozených navzájem nesoudělných čísel platí $f(ab) = f(a)f(b)$. Funkce je *úplně multiplikativní*, pokud $f(ab) = f(a)f(b)$ platí pro každou dvojici přirozených čísel.

Proč je multiplikativita aritmetických funkcí z několika důvodů velmi příjemná? Z několika důvodů. Jedním z nich je to, že je funkce jednoznačně určená svými hodnotami v mocninách prvočísel. Pomocí matematické indukce totiž snadno dostaneme intuitivní vzoreček

$$f(p_1^{\alpha_1} \cdots p_r^{\alpha_r}) = f(p_1^{\alpha_1}) \cdots f(p_r^{\alpha_r}).$$

Když tedy potřebujeme spočítat hodnotu v čísle n, stačí jej rozložit na prvočísla, zjistit hodnoty v mocninách prvočísel a využít tohoto vzorečku. Obdobně, když chceme ukázat rovnost dvou multiplikativních funkcí, stačí dokázat, že se rovnají ve všech mocninách prvočísel.

Pro úplně multiplikativní funkce je situace podobná. Pro výpočet hodnoty n stačí znát hodnoty v jednotlivých prvočíslech z rozkladu (úplně multiplikativní funkce je totiž multiplikativní a navíc platí $f(p^k) = f(p)^k$). Aby se dvě úplně multiplikativní funkce rovnaly, stačí, aby měly stejné hodnoty v prvočíslech.

Cvičení. Uvědom si, že funkce I, u, N a μ jsou multiplikativní. Které z nich jsou multiplikativní úplně?

U dvou důležitých funkcí už jsme si multiplikativitu nenápadně dokázali – u Eulerovy funkce φ (již v prvním díle) a Legendreova symbolu L_p (ve druhém díle).

Cvičení. Dokaž, že pokud je f multiplikativní funkce, tak $f(1) = 1$.

Asi nikoho nepřekvapí, že jsou-li f a g multiplikativní funkce a h je definovaná jako $h(n) = f(n) \cdot g(n)$, tak je i h multiplikativní. Ale opravdové kouzlo a sílu multiplikativity poodkrývá následující tvrzení.

Tvrzení. (Konvoluce zachovává multiplikativitu) *Pokud jsou f a g multiplikativní, pak je multiplikativní i $f * g$.*

Důkaz. Nechť $h = f * g$ a m, n jsou dvě nesoudělná čísla. Pak

$$h(mn) = \sum_{d \mid mn} f(d)\, g\Big(\frac{mn}{d}\Big).$$

[14] Extrémně významnou.

Každý dělitel d čísla mn se dá napsat ve tvaru $d = ab$, kde $a \mid m$, $b \mid n$. Navíc platí $(a, b) = 1$, $(\frac{m}{a}, \frac{n}{b}) = 1$. Naopak každá taková dvojice a, b odpovídá právě jednomu děliteli d. Proto se rovnají sumy

$$\sum_{d \mid mn} f(d)\, g\Big(\frac{mn}{d}\Big) = \sum_{\substack{a \mid m \\ b \mid n}} f(ab)\, g\Big(\frac{mn}{ab}\Big).$$

Na pravé straně jsme získali dvojitou sumu, ze které vyrobíme součin sum, podobně jako jsme si to ukazovali v úvodní kapitole.

$$\begin{aligned} h(mn) &= \sum_{\substack{a \mid m \\ b \mid n}} f(ab)\, g\Big(\frac{mn}{ab}\Big) \\ &= \sum_{b \mid n} \sum_{a \mid m} \Big(f(a)\, f(b)\, g\Big(\frac{m}{a}\Big)\, g\Big(\frac{n}{b}\Big)\Big) \\ &= \sum_{b \mid n} \Big(f(b)\, g\Big(\frac{n}{b}\Big) \cdot \Big(\sum_{a \mid m} f(a)\, g\Big(\frac{m}{a}\Big)\Big)\Big) \\ &= \Big(\sum_{a \mid m} f(a)\, g\Big(\frac{m}{a}\Big)\Big)\Big(\sum_{b \mid n} f(b)\, g\Big(\frac{n}{b}\Big)\Big) \\ &= h(m)\, h(n). \end{aligned}$$

Získali jsme novou zbraň, jak o funkcích ukazovat, že jsou multiplikativní.

Tvrzení. *Funkce τ (počet dělitelů) a σ (součet dělitelů) jsou multiplikativní.*[15]

Důkaz. Tvrzení se samozřejmě dá dokázat z definice multiplikativity, ale vyžaduje to netriviální množství počítání a úprav. S tím, co jsme si dokázali o konvoluci, se tvrzení vzdá.

Stačí si uvědomit, že $\tau(n) = \sum_{d \mid n} 1$ je sumární funkce jednotky u, tedy $\tau = u * u$. Podobně $\sigma(n) = \sum_{d \mid n} d$ je sumární funkce „nudy“ N, tedy $\sigma = N * u$. Funkce u a N jsou multiplikativní a díky tomu, že konvoluce zachovává multiplikativitu, jsou i funkce τ a σ multiplikativní.

Poznámka. Nyní již snadno dokážeme, že pro $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ platí

$$\sigma(n) = \frac{p_1^{\alpha_1+1}}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1}}{p_2 - 1} \cdots \frac{p_r^{\alpha_r+1}}{p_r - 1}.$$

Cvičení. Dokaž si, že součet dělitelů závisí na počtu dělitelů takto:

$$\sigma(n) = \sum_{d \mid n} \tau(d)\, \varphi\Big(\frac{n}{d}\Big).$$

Cvičení. Uvědom si, že konvoluce nezachovává úplnou multiplikativitu.

Návod. $\tau = u * u$.

Z toho důvodu je multiplikativita důležitější a zajímavější než úplná multiplikativita.[16] To, že je funkce multiplikativní úplně, už je jen taková třešnička na dortu.[17] Na druhou stranu se tato vlastnost občas chová nadstandardně pěkně. Tak je tomu například u Dirichletových inverzí.

[15] Platí dokonce zobecněná věta: součet k-tých mocnin dělitelů čísla n, neboli $\sigma_k(n) = \sum_{d \mid n} d^k$, je multiplikativní.

[16] Přestože definice úplné multiplikativity se zdá být přirozenější.

[17] Nebo hřebíček do rakve.

Definice. Nechť f je aritmetická funkce taková, že $f(1) \neq 0$. Potom funkci g nazveme *Dirichletovou inverzí* k f, pokud $f * g = g * f = I$. Obvykle ji značíme f^{-1}.

Dá se ukázat, že pro každou funkci existuje právě jedna Dirichletova inverze, my to ale dělat nebudeme. Také se dá odvodit ne úplně pěkný rekurentní vztah pro hodnoty funkce f^{-1} v závislosti na funkci f. My díky Dirichletovým inverzím dostaneme zajímavou charakterizaci úplně multiplikativních funkcí. Drž si klobouk!

Tvrzení. *Nechť f je multiplikativní. Pak f je úplně multiplikativní, právě když*

$$f^{-1}(n) = \mu(n) f(n) \quad \text{pro každé přirozené } n.$$

Cvičení. (těžké) Zkus si tvrzení dokázat.

Návod. Pro jednu implikaci využij tvrzení $\sum_{d|n} \mu(d) = I(d)$. V druhé implikaci si uvědom, jak vypadá $\mu(p^k)$, a dokaž $f(p^\alpha) = f(p)^\alpha$.

Bonusy na závěr

Jednoduchou aplikací Dirichletovy konvoluce je následující překvapivé tvrzení, které říká, jak obrátit vztah „f je sumární funkce g“.

Tvrzení. (Möbiova inverzní formule) *Rovnosti*

$$f(n) = \sum_{d|n} g(d)$$

a

$$g(n) = \sum_{d|n} f(d)\, \mu\Big(\frac{n}{d}\Big)$$

jsou ekvivalentní.

Důkaz. Víme, že první rovnost znamená $f = g * u$. Vynásobením funkcí μ dostáváme $f * \mu = (g * u) * \mu = g * (u * \mu) = g * I = g$, což je druhá rovnost. Když naopak tuto rovnost vynásobíme funkcí u, dostaneme opět první rovnost.

Vše, čím jsme se dosud v seriálu zabývali, bylo konečné (a tedy do jisté míry omezené). Pojďme se tedy na chvilku odpoutat od nudné reality a vrhněme se do nekonečného vesmíru plného nekonečných řad.

S nějakou nekonečnou řadou ses již pravděpodobně setkal(a). Například s krotkou řadou

$$1 + \frac{1}{2} + \cdots + \frac{1}{2^k} + \cdots = \sum_{k=0}^{\infty} 2^{-k},$$

která má konečný součet 2. Naproti tomu řada

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots$$

má součet nekonečno.[18]

[18] Vyšetřování, zda má nekonečná řada konečný součet, není snadné a my se jím nebudeme zabývat.

Obrovské využití v teorii čísel ale mají poněkud divočejší řady, kupříkladu řady tvaru

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \quad \text{pro pevné } s > 1.$$

Dá se ukázat, že pro $s > 1$ má tato řada konečný součet, který označujeme $\zeta(s)$.[19] Platí například známý vztah

$$\zeta(2) = \frac{\pi^2}{6}.$$

Pořád je Ti to málo? Nám také. Pojďme si tyto řady ještě zobecnit.

Definice. Nechť a je aritmetická funkce. Pak

$$D(a, s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s},$$

nazveme *Dirichletovou řadou* funkce a.

Příkladem jsou tyto řady:

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)},$$
$$\sum_{n=1}^{\infty} \frac{\tau(n)}{n^s} = \zeta(s)^2,$$
$$\sum_{n=1}^{\infty} \frac{\sigma(n)}{n^s} = \zeta(s) \cdot \zeta(s-1).$$

Tvrzení. *Platí*

$$D(a * b, s) = D(a, s) \cdot D(b, s).$$

Náznak důkazu. Představ si, jak se postupně roznásobuje pravá strana. Pokud dáš k sobě členy, které mají ve jmenovateli n^s pro nějaké n, tak zjistíš, že v čitateli bude přesně

$$\sum_{d|n} a(d) \cdot b\Big(\frac{n}{d}\Big).$$

Tato úvaha opravdu funguje i pro nekonečné řady, jen je potřeba ještě trocha teorie a formalit, což překračuje rámec seriálu.

Cvičení. S pomocí tvrzení si dokaž tři předchozí identity.

Cvičení. (těžké) Nahlédni, že asi platí

$$\zeta(s) = \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{1}{p^s}},$$

kde v součinu násobíme přes všechna prvočísla.

Návod. Rozepiš si $\frac{1}{1-1/p^s}$ jako geometrickou řadu

$$1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots.$$

[19] Jedná se o známou Riemannovu zeta funkci, o které hovoří nejslavnější nevyřešený matematický problém – Riemannova hypotéza.

Jak dostaneš na pravé straně $1/n^s$? Zkus si n rozložit na prvočísla.

Cvičení. (těžké) Dokaž, že

$$\frac{6}{\pi^2} < \frac{\varphi(n) \cdot \sigma(n)}{n^2} < 1.$$

Návod. Napiš si vzorečky pro $\varphi(n)$ a $\sigma(n)$, z obou vytkni n a využij předchozí cvičení.

Závěr

Pokud ses dočetl(a) až sem, chtěli bychom Ti pogratulovat a poděkovat za to, že jsi našemu seriálu udržel(a) přízeň. Pokud Tě téma zaujalo, v příštích komentářích najdeš seznam další literatury, mimo jiné zdroje, ze kterých jsme při psaní seriálu čerpali.

Dále bychom rádi poděkovali našemu jazykovému korektorovi Kubovi a TEXaři Olinovi za to, že po nás celý text důkladně pročítali, a za trpělivost, kterou s námi měli. Rovněž děkujeme i ostatním organizátorům, kteří pomohli výsledný text doladit.