VII. kapitola. Využití principu inkluze a exkluze v teorii čísel

In: Antonín Vrba (author): Kombinatorika. (Czech). Praha: Mladá fronta, 1980. pp. 57–63.

Persistent URL: http://dml.cz/dmlcz/403970

VYUŽITÍ PRINCIPU INKLUZE A EXKLUZE V TEORII ČÍSEL*)

V teorii čísel hraje významnou roli tzv. Eulerova**) funkce $\varphi(n)$, která přiřazuje každému přirozenému číslu $n > 1$ počet všech přirozených čísel, která jsou menší než n a přitom s n nesoudělná. Tak např. $\varphi(28) = 12$, neboť z čísel menších než 28 je s ním nesoudělných právě 12 čísel, totiž 1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27. Známá Fermatova***) věta tvrdí: *Je-li a celé číslo, které není dělitelné prvočíslem p, pak a^{p-1} dává při dělení prvočíslem p zbytek* 1. L. Euler zobecnil tuto větu pro všechna přirozená čísla $p > 1$ a v ní se pak setkáme s Eulerovou funkcí:

Je-li a celé číslo a p přirozené číslo nesoudělné s a, potom při dělení $a^{\varphi(p)}$ číslem p zbude 1. (Je-li p prvočíslo, redukuje se Eulerova věta na Fermatovu větu, neboť pro prvočíslo p platí $\varphi(p) = p - 1$; žádné z čísel 1, 2, ..., $p - 1$ totiž není soudělné s prvočíslem p.)

Nebudeme zde tyto teorie dále rozvíjet a soustředíme se na problém, jak pro dané přirozené číslo $n > 1$ spočíst příslušnou hodnotu $\varphi(n)$. Je-li n velké, dá vyhledání

*) Na tuto kapitolu se dále nenavazuje.

**) L. Euler (1707—1783) — proslulý matematik švýcarského původu. Svými více než osmi sty pracemi ovlivnil téměř všechny oblasti matematiky a teoretické mechaniky.

***) P. Fermat (1601—1665) — francouzský právník, který se úspěšně zabýval matematikou a optikou.

všech menších a s n nesoudělných čísel hodně práce. Pokud však známe všechna prvočísla $p_1, p_2, \ldots, p_k$ vyskytující se v rozkladu čísla n na prvočinitele (jejich násobnosti potřebovat nebudeme), pomůže princip inkluze a exkluze.

Pro každé $i \in \{1, 2, \ldots, k\}$ označme M_i množinu všech přirozených čísel nejvýše rovných n, která jsou dělitelná prvočíslem p_i. Množina $M_1 \cup M_2 \cup \ldots \cup M_k$ obsahuje všechna přirozená čísla menší než n, která jsou dělitelná některým z prvočísel $p_1, p_2, \ldots, p_k$, tedy která jsou soudělná s číslem n. Je tedy

$$|M_1 \cup M_2 \cup \ldots \cup M_n| = n - \varphi(n).$$

Buď $\emptyset \neq \{j_1, j_2, \ldots, j_r\} \subset \{1, 2, \ldots, k\}$. Množina $M_{j_1} \cap \cap M_{j_2} \cap \ldots \cap M_{j_r}$ obsahuje všechna přirozená čísla nejvýše rovná n, která jsou dělitelná každým z prvočísel $p_{j_1}, p_{j_2}, \ldots, p_{j_r}$ a tedy i jejich součinem $p_{j_1} p_{j_2} \ldots p_{j_r}$. Je jich

$$|M_{j_1} \cap M_{j_2} \cap \ldots \cap M_{j_r}| = \frac{n}{p_{j_1} p_{j_2} \ldots p_{j_r}}.$$

Podle principu inkluze a exkluze dostáváme

$$n - \varphi(n) = \Sigma(-1)^{r+1} \frac{n}{p_{j_1} p_{j_2} \ldots p_{j_r}}$$

neboli

$$\varphi(n) = n\left(1 + \Sigma(-1)^r \frac{1}{p_{j_1} p_{j_2} \ldots p_{j_r}}\right), \tag{18}$$

kde se sčítá přes všechny neprázdné podmnožiny $\{j_1, j_2, \ldots, j_r\} \subset \{1, 2, \ldots, k\}$. Výraz v závorce na pravé straně však vznikne, jak se snadno přesvědčíme, roznásobením součinu

$$\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).$$

Odvodili jsme tak vzorec

$$(19)\quad \varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_k}\right).$$

Vraťme se k příkladu, který jsme uvedli na začátku: V rozkladu čísla 28 na prvočinitele se vyskytují prvočísla 2 a 7. Je tedy

$$\varphi(28)=28\left(1-\frac{1}{2}\right)\left(1-\frac{1}{7}\right)=12,$$

což souhlasí s tím, co jsme zjistili na začátku.

U velkých čísel je význam vzorce zvlášť patrný ve srovnání s bezprostředním hledáním nesoudělných čísel. Například

$$\varphi(221\,728)=\varphi(2^5.13^2.41)=$$

$$=221\,728\left(1-\frac{1}{2}\right)\left(1-\frac{1}{13}\right)\left(1-\frac{1}{41}\right)=99\,840.$$

Obraťme dále svou pozornost k jiné důležité funkci, která se studuje v číselné teorii. Je to funkce $\pi(n)$, která přiřazuje každému přirozenému číslu n počet všech prvočísel, která jsou nejvýše rovna n. Průběh této funkce tedy vlastně vyjadřuje rozložení prvočísel mezi přirozenými čísly. To je jeden ze základních problémů teorie čísel, jehož zkoumání bylo v průběhu historie matematiky věnováno nemálo úsilí. Leccos se vyjasnilo, ale dost obtížných otázek zůstává ještě otevřených.

Nejprve si připomeňme, že všechna prvočísla menší než dané $n > 1$ lze najít postupem zvaným Eratosthe-

novo*) síto. Spočívá v tom, že se z čísel 2, 3, ..., n nejprve vynechají všechny násobky čísla 2 větší než 2. Pak se vynechají všechny násobky čísla 3 větší než 3 atd.; v k-tém kroku se tedy ponechá k-té dosud nevynechané číslo odleva a vynechají se všechny jeho další násobky. Nakonec ovšem zbudou právě všechna prvočísla nejvýše rovná n, přičemž stačilo provést $[\sqrt{n}]$ kroků. Každé složené číslo nejvýše rovné n je totiž dělitelno některým prvočíslem nejvýše rovným $\sqrt{n}$. Idea Eratosthenova síta se sleduje i v následující úvaze.

Buď $n > 1$ přirozené číslo a položme $k = \pi([\sqrt{n}])$. Pro každé $i \in \{1, 2, \ldots, k\}$ označme M_i množinu všech přirozených čísel nejvýše rovných n, která jsou dělitelná i-tým (v přirozeném pořadí) prvočíslem p_i. Množina $M_1 \cup M_2 \cup \ldots \cup M_k$ obsahuje všechna složená čísla nejvýše rovná n a kromě nich ještě právě prvních k prvočísel. Obsahuje tedy kromě čísla 1 a prvočísel větších než $\sqrt{n}$ všechna přirozená čísla nejvýše rovná n. Je tedy

$$|M_1 \cup M_2 \cup \ldots \cup M_k| = n - 1 - \pi(n) + \pi([\sqrt{n}]).$$

Je-li $\emptyset \neq \{j_1, j_2, \ldots, j_r\} \subset \{1, 2, \ldots, k\}$, obsahuje množina $M_{j_1} \cap M_{j_2} \cap \ldots \cap M_{j_r}$ všechna přirozená čísla nejvýše rovná n, která jsou dělitelná každým z prvočísel $p_{j_1}, p_{j_2}, \ldots, p_{j_r}$ a tedy i jejich součinem $p_{j_1} p_{j_2} \ldots p_{j_r}$. Je tedy

$$|M_{j_1} \cap M_{j_2} \cap \ldots \cap M_{j_r}| = \left[\frac{n}{p_{j_1} p_{j_2} \ldots p_{j_r}}\right].$$

*) Eratosthenes z Kyreny (276—194 př. n. l.) — řecký matematik a astronom.

Podle principu inkluze a exkluze dostáváme

$$n - 1 - \pi(n) + \pi([\sqrt{n}]) = \Sigma\,(-1)^{r+1}\left[\frac{n}{p_{i_1}p_{i_2}\cdots p_{i_r}}\right]$$

neboli

$$(20)\quad \pi(n) = n - 1 + \pi([\sqrt{n}]) + \Sigma(-1)^r\left[\frac{n}{p_{i_1}p_{i_2}\cdots p_{i_r}}\right],$$

kde se sčítá přes všechny neprázdné podmnožiny

$$\{j_1, j_2, \ldots, j_r\} \subset \{1, 2, \ldots, \pi([\sqrt{n}])\}.$$

Vyjádřili jsme tedy $\pi(n)$ pomocí hodnoty funkce pro podstatně menší proměnnou, totiž pomocí $\pi([\sqrt{n}])$. Za to jsme samozřejmě museli něco zaplatit: Potřebujeme znát ještě také všech $\pi([\sqrt{n}])$ prvních prvočísel (tedy nejen jejich počet) a musíme spočíst příslušné zlomky.

Určeme pro ilustraci $\pi(120)$. Je $[\sqrt{120}] = 10$ a prvočísla menší než 10 jsou 2, 3, 5, 7. Vypočítáme $2^4 - 1$ zlomků

$$\left[\frac{120}{2}\right] = 60,\ \left[\frac{120}{3}\right] = 40,\ \left[\frac{120}{5}\right] = 24,\ \left[\frac{120}{7}\right] = 17,$$

$$\left[\frac{120}{2.3}\right] = 20,\ \left[\frac{120}{2.5}\right] = 12,\ \left[\frac{120}{2.7}\right] = 8,\ \left[\frac{120}{3.5}\right] = 8,$$

$$\left[\frac{120}{3.7}\right] = 5,\ \left[\frac{120}{5.7}\right] = 3,$$

$$\left[\frac{120}{2.3.5}\right] = 4,\left[\frac{120}{2.3.7}\right] = 2,\left[\frac{120}{2.5.7}\right] = 1,\left[\frac{120}{3.5.7}\right] = 1,$$

$$\left[\frac{120}{2.3.5.7}\right] = 0.$$

Dostáváme

$$\pi(120) = 120 - 1 + 4 - (60 + 40 + 24 + 17) + \\ + (20 + 12 + 8 + 8 + 5 + 3) - \\ - (4 + 2 + 1 + 1) = 30.$$

K praktickému výpočtu hodnot funkce $\pi(n)$ se, jak je vidět, vzorec (20) příliš nehodí, méně práce dá Eratosthenovo síto. Vzorec má však význam pro teorii.

Cvičení

7.1 Dokažte, že pro každá dvě přirozená čísla $m > 1$, $n > 1$ platí

$$\varphi(m)\,\varphi(n) \leqq \varphi(mn).$$

Kdy nastane rovnost?

7.2 Dokažte, že pro $n > 2$ je $\varphi(n)$ sudé číslo.

7.3 Kolik z čísel 1, 2, ..., 100 000 je mocninou jiného přirozeného čísla?

7.4 V teorii čísel se pracuje také s Möbiovou*) funkcí $\mu(n)$, která je definována pro všechna přirozená čísla n takto: Pokud se v rozkladu čísla $n > 1$ v součin prvočinitelů nevyskytuje žádné prvočíslo ve vyšší než první mocnině, klade se $\mu(n) = (-1)^v$, kde v je počet prvočinitelů. Pro ostatní n se klade $\mu(n) = 0$ s jedinou výjimkou $\mu(1) = 1$. Dokažte

a) $\Sigma\mu(d) = 0$, sčítá-li se přes všechny kladné dělitele d přirozeného čísla $n > 1$.

b) $\varphi(n) = n\,\Sigma\frac{\mu(d)}{d}$, sčítá-li se přes všechny kladné dělitele d přirozeného čísla $n > 1$.

---

*) A. F. Möbius (1790—1868) — německý astronom a matematik. Vynikl zejména v geometrii.

c) $\pi(n) = \pi([\sqrt{n}]) - 1 + \Sigma\mu(d)\left[\frac{n}{d}\right]$, sčítá-li se přes všechny kladné dělitele d součinu všech prvočísel nejvýše rovných $\sqrt{n}$.

d) $\Sigma\mu(d)\left[\frac{n}{d}\right] = 1$, sčítá-li se přes všechny kladné dělitele d součinu všech prvočísel nejvýše rovných přirozenému číslu $n > 1$.