BRněnský KOrespondenční Seminář

XXXI. ročník
2024/2025

Pomocný text ke 2. sérii

ZBYTKY

autor: *Áďa Heroudková*

1 Zbytky po dělení

1.1 Motivace

Jedním ze základních pojmů z teorie čísel je dělitelnost a s tím spojené zbytkové třídy a kongruence. Jsou to důležité pojmy, nejen v matematické olympiádě, ale i v teoretické matematice.

U čísel nás totiž nemusí pouze zajímat, jaká jiná čísla je dělí, ale i jaké zbytky dávají po dělení dalšími čísly. Příkladem nám můžou být lichá čísla, jejichž hlavní vlastností je, že dávají zbytek jedna po dělení dvěma.

Jak nám může pomoc zkoumání zbytků po dělení při řešení příkladů?

Příklad 1: Najděte všechny dvojice přirozených čísel k, l, které splňují rovnici:

$$(3k+1)^2 = 3l+2$$

.

Řešení: Rozepišme si rovnici:

$$9k^2 + 6k + 1 = 3l + 2$$

Vidíme, že číslo na levé straně rovnice bude vždy dávat zbytek jedna po dělení třemi a číslo na pravé straně rovnice dává vždy zbytek dva po dělení třemi. Tudíž nemůže existovat žádná dvojice přirozených čisel, která by splňovala tuto rovnici.

S podobnými rovnicemi bychom si mohli hrát do nekonečna, ale abychom byli schopni řešit komplikovanější příklady, hodí se nám naučit se základní terminologii a základní práci se zbytky.

1.2 Zbytkové třídy

Když si vezmeme nějaké přirozené číslo n, můžeme si rozdělit všechny přirozené (dokonce i celé) čísla do množin, podle toho, jaký dávají zbytek po dělení n. Více zkušení by řekli: Můžeme všechna celá čísla rozdělit do zbytkových tříd, podle toho jaký zbytek dávají modulo n.

Máme tedy n tříd, každá symbolizující jeden možný zbytek, množina těchto n tříd se často značí $\mathbb{Z}_n$ nebo $\mathbb{Z}/n$. Na těchto třídách dokonce můžeme zavést operace. Sečteme-li například dvě libovolná čísla, které dávají zbytek 1 modulo 3, pak dostaneme číslo, které dává zbytek 2 modulo 3.

Pojďme si tyto věci korektně zadefivat.

Definice: Mějme celá čísla a, b a přirozené číslo n. Řekneme, že a je kongruentní s b modulo n, psáno: $a \equiv b \mod n$, pokud n dělí $(a-b)$.

Poznámka: Množinu čísel, které jsou kongruentní s celým číslem a modulo n značíme $[a]_n$. Takových různých množin kongruetních čísel modulo n je přesně n. Říkáme jim zbytkové třídy a často je značíme $[0]_n$, $[1]_n$,..., $[n-1]_n$.

Každé celé číslo si totiž můžeme zapsat ve tvaru

$$a = kn + n',$$

kde k je celé číslo a n' je nezáporné celé číslo menší než n (zmiňovaný zbytek). Tento zápis je dokonce jednoznačný. Dvě čísla dávají stejný zbytek modulo n pokud mají v zápisu stejné n'. Tedy jejich rozdíl $(k_1 n + n') - (k_2 n + n') = (k_1 - k_2)n$ je dělitelný n. Proto každé číslo můžeme přiřadit do zbytkové třídy $[n']_n$.

Tento zápis nám pomůže pochopit operace na kongruencích (zbytkových třídách).

Věta 1: Nechť $a \equiv b \mod n$, $c \equiv d \mod n$, potom platí:

- $a + c \equiv b + d \mod n$
- $a - c \equiv b - d \mod n$
- $a \cdot d \equiv b \cdot d \mod n$
- nechť k je libovolné nezáporné celé číslo: $a^k \equiv b^k \mod n$

Důkaz: Rozepišme si čísla a, b, c, d následovně:

$$a = fn + n',$$
$$b = gn + n',$$
$$c = hn + n'',$$
$$d = in + n'',$$

kde f, g, h, i jsou celá čísla a n', n'' jsou nezáporná celá čísla menší než n.

Tedy platí:

$$a + c = (f + h)n + (n' + n'')$$
$$b + d = (g + i)n + (n' + n'').$$

Obě čísla tedy budou dávat stejný zbytek po dělení n.

Obdobný argument můžeme provést pro násobení, odčítání a mocnění. Pokud mi to nevěříte doporučuji zkusit si to propočítat.

Dělení je komplikovanější, ne vždy ho totiž můžeme provést. Na řešení této série není potřeba, ale pokud by vás to zajímalo, tak si ho zkuste promyslet či vyhledat.

Pojďme si na procvičení ukázat, jak můžeme využít vlastnost zmiňovaného mocnění v praxi:

Příklad 2: Jaký zbytek dává 13^6 po dělení 15?

Řešení: Rozepišme si to pomocí kongruencí:

$$13 \equiv -2 \mod 15$$

$$13^6 \equiv (-2)^6 \mod 15$$

$$(-2)^6 \equiv (-2)^4 \cdot (-2)^2 \equiv 16 \cdot 4 \mod 15$$

$$16 \equiv 1 \mod 15 \longrightarrow (-2)^6 \equiv 1 \cdot 4 \equiv 4 \mod 15$$

Na ulehčení počítání nám slouží takzvaná Čínská zbytková věta.

Věta 2: Předpokládejme, že $m_1, m_2, \ldots, m_r$ jsou navzájem po dvou nesoudělná přirozená čísla, $m_i \geq 2$ pro $i = 1, \ldots, r$. Potom každá soustava rovnic:

$$x \equiv a_1 \mod m_1$$

$$x \equiv a_2 \mod m_2$$

$$\ldots$$

$$x \equiv a_r \mod m_r$$

má řešení x, které je určeno jednoznačně modulo $M = m_1 \cdot m_2 \cdot \cdots \cdot m_r$.

Jednoduché použití čínské zbytkové věty je například:

Příklad 3: Určete jaký zbytek dává číslo 4^{100} po dělení 15.

Řešení: Čísla 3 a 5 jsou nesoudělná. Můžeme se tedy podívat na číslo 4^{100} zvlášť modulo 3 a 5.

$$4 \equiv 1 \mod 3$$

$$4^{100} \equiv 1^{100} \equiv 1 \mod 3$$

$$4 \equiv -1 \mod 5$$

$$4^{100} \equiv (-1)^{100} \equiv 1 \mod 5$$

Z Čínské zbytkové věty víme, že existuje pouze jedno číslo modulo 15, které je 1 modulo 3 i 1 modulo 5. Takovým zbytkem je 1 modulo 15.

1.3 Kvadratické zbytky

Můžeme zkoumat vlastnosti různých typů zbytků. V téhle sekci se zaměříme na ty takzvané kvadratické, neboť jejich vlastnosti se hodí k řešení mnohých rovnic či olympiádních úloh.

Definice: Číslo a nazveme kvadratickým zbytkem modulo n, pokud existuje celé číslo x takové, že $x^2 \equiv a \mod n$.

Pro některé může být překvapivé, že ne všechna čísla jsou kvadratickým zbytkem. Když je nějaké číslo kvadratickým zbytkem, všechna čísla, co jsou s ním ve stejné zbytkové třídě, jsou též kvadratickým zbytkem. Můžeme se pak zabývat otázkou kolik existuje různých zbytkových tříd modulo n obsahující kvadratické zbytky. O číslech, které nejsou kvadratickými zbytky modulo n, mluvíme jako o kvadratických nezbytcích modulo n.

Příklad 4: Najděte všechny třídy obsahující kvadratické zbytky modulo 4.

Řešení: Situaci si můžeme rozdělit do čtyř případů:

- $x \equiv 0 \mod 4$: Potom $x^2 \equiv 0 \mod 4$
- $x \equiv 1 \mod 4$: Potom $x^2 \equiv 1 \mod 4$
- $x \equiv 2 \mod 4$: Potom $x^2 \equiv 4 \equiv 0 \mod 4$
- $x \equiv 3 \mod 4$: Potom $x^2 \equiv 3^2 \equiv 1 \mod 4$.

Jak můžeme vidět, tak kvadratickými zbytky jsou právě prvky třídy $[0]_4$ a $[1]_4$. Tím, že jsme prošli všechny možnosti druhých mocnin, tak víme, že třídy $[2]_4$ a $[3]_4$ nemůžou obsahovat kvadratické zbytky.

Z toho důvodu, že druhé mocniny můžou dávat zbytek pouze 0 nebo 1 modulo 4, se občas hodí dívat na rovnice s druhými mocninami modulo 4. Případně modulo vyšší mocniny dvojky, protože mají taky velmi málo tříd s kvadratickými zbytky.

Též se kvadratické zbytky chovají velice pěkně modulo lichá prvočísla. Pokud by vás to zajímalo více doporučuji si vyhledat zákon kvadratické reciprocity. My si tady zmíníme jen pár zajímavých vlastností.

Věta 3: Nechť p je liché prvočíslo, potom existuje právě $\frac{p+1}{2}$ tříd modulo p obsahující kvadratické zbytky.

Kdybychom nulu nepovažovali za kvadratický zbytek bylo by jich $\frac{p-1}{2}$.

Věta 4: Mějme liché prvočíslo p:

- Pokud je $p \equiv 1 \mod 4$, potom pokud a je kvadratický zbytek modulo p je i $-a$ kvadratický zbytek. Naopak pokud je b kvadratický nezbytek, je i $-b$ kvadratický nezbytek.
- Pokud je $p \equiv 3 \mod 4$, potom pokud je a kvadratický zbytek modulo p je $-a$ kvadratický nezbytek. A naopak, pokud je b kvadratický nezbytek je $-b$ kvadratický zbytek.

1.4 Závěr

Jak jsme mohli vidět zbytky po dělení a kongruence mají spoustu zajímavých vlastností a dá se s nimi pěkně pracovat. Proto se nám často vyplatí je používat při řešení příkladů z teorie čísel.