Teorie čísel: Cvičení 8 – výsledky, nápovědy, vzorová řešení

Simona Hlavinková, email: simonkahlavinkova@gmail.com

Nápovědy:

4. Jaký zbytek mohou a^2 a b^2 dávat modulo 3?

8. Stačí si uvědomit, že zadání se vlastně ptá, kdy je -7 kvadratický zbytek modulo p. Postupujte jako v úloze 5.

9. Zkuste si uvědomit, co se stane s množinou všech kvadratických zbytků, když je vynásobíme nějakým fixním kvadratickým zbytkem. Nejde pomocí toho zkoumaný součet vyjádřit dvěma různými způsoby, a ty porovnat? Alternativa: Zkuste se zamyslet nad použitím primitivního prvku; třeba to k něčemu bude.

10. Nejprve si uvědomíme, že $ka+b$ ve skutečnosti neiteruje přes nic jiného než přes všechny prvky $\mathbb{Z}_p$. Pak už se jenom stačí zamyslet nad počtem zbytků a nezbytků.

11. Nejedná se vlastně o nic jiného než o řešení kongruence $x^2 \equiv y^2 + 1 \pmod p$. Ta je splněná právě tehdy, když $x-y$ a $x+y$ jsou navzájem inverzní prvky. Zamyslete se, jak obecně vypadají všechny dvojice navzájem inverzních prvků v $\mathbb{Z}_p^*$ a z toho úlohu dořešte.

Výsledky:

Poznámka: Náhodou se stalo, že skoro všechny konkrétní spočtené Legendreovy symboly ze cvičení vyšly -1. To je skutečně náhoda :)

-2. Modulo 4: $\{0,1\}$, modulo 7: $\{0,1,2,4\}$.

-1. Všechny vyjdou -1.

0.
$$\left(\frac{3}{p}\right) = \begin{cases} \text{nedefinováno} & \text{pokud } p = 2, \\ 0 & \text{pokud } p = 3, \\ 1 & \text{pokud } p \equiv \pm 1 \pmod{12}, \\ -1 & \text{jinak (tj. pokud } p \equiv \pm 5 \pmod{12}). \end{cases}$$

1. Modulo 8: $\{0,1,4\}$, modulo 9: $\{0,1,4,7\}$, modulo 17: $\{0,1,2,4,8,9,13,15,16\}$.

2. $\left(\frac{17}{5}\right) = \left(\frac{5}{17}\right) = -1$

3. Všechny vyjdou -1.

5.
$$\left(\frac{7}{p}\right) = \begin{cases} \text{nedefinováno} & \text{pokud } p = 2, \\ 0 & \text{pokud } p = 7, \\ 1 & \text{pokud } p \equiv 1,3,9,19,25,27 \pmod{28}, \\ -1 & \text{jinak (tj. pokud } p \equiv 5,11,13,15,17,23 \pmod{28}). \end{cases}$$

$$\left(\frac{13}{p}\right) = \begin{cases} \text{nedefinováno} & \text{pokud } p = 2, \\ 0 & \text{pokud } p = 13, \\ 1 & \text{pokud } p \equiv 1,3,4,9,10,12 \pmod{13}, \\ -1 & \text{jinak (tj. pokud } p \equiv 2,5,6,7,8,11 \pmod{13} \text{ a } p \neq 2). \end{cases}$$

6. Uvažte modulo 8.

7. Platí to právě pro $p = 2$ a $p \equiv 1 \pmod 4$. Přepište si zadání do řeči Legendreových symbolů a uvažte jejich multiplikativitu. Kdy je -1 kvadratický zbytek modulo p?

8. Řešením je $p = 2$, $p = 7$ a všechna prvočísla tvaru $p \equiv 1, 2, 4 \pmod 7$.

Vybraná vzorová řešení:

-2.) Uvědomme si, že $(an + b)^2 = a^2n^2 + 2abn + b^2 \equiv b^2 \pmod n$. Když tedy chceme spočítat všechny kvadratické zbytky modulo n, tak se stačí ve skutečnosti omezit jenom na druhé mocniny prvků v okruhu $\mathbb{Z}_n$. Stejně tak si jde uvědomit, že $x^2 \equiv (-x)^2 \pmod n$, tedy stačí mocnit jenom polovinu prvků.

Například pro $n = 4$ tak dostaneme právě zbytky $0^2 \equiv 0$, $1^2 \equiv 1$ a $2^2 \equiv 0 \pmod 4$. Podobně pro $n = 7$ dostaneme zbytky $0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 4$ a $3^2 \equiv 2 \pmod 7$.

0.) Rádi bychom použili kvadratickou reciprocitu a převedli úlohu na problém s určením $\left(\frac{p}{3}\right)$, což je daleko přístupnější. K jejímu použití ale potřebujeme, aby p bylo liché prvočíslo různé od 3. Na začátek tedy zvlášť vyřešíme případy $p = 2$ a $p = 3$. Přímo z definice platí $\left(\frac{3}{3}\right) = 0$ a $\left(\frac{3}{2}\right)$ není definováno.

Nyní můžeme předpokládat $p \neq 2, 3$. Použitím kvadratické reciprocity dostáváme[1]

$$\left(\frac{3}{p}\right) = (-1)^{\frac{3-1}{2}\frac{p-1}{2}} \left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right).$$

Jak je známo (a jde jednoduše ověřit), tak $(-1)^{\frac{p-1}{2}}$ je rovno 1 pro $p \equiv 1 \pmod 4$ a -1 pro $p \equiv -1 \pmod 4$. Podobně (z toho, jak vypadají kvadratické zbytky modulo 3) dostáváme, že $\left(\frac{p}{3}\right) = 1$ pro $p \equiv 1 \pmod 3$ a $\left(\frac{p}{3}\right) = -1$ pro $p \equiv 2 \pmod 3$. Z Čínské zbytkové věty tak máme, že hodnota výrazu napravo je tak jednoznačně určená tím, jaký zbytek dává p modulo $12 = 3 \cdot 4$.

Pokud tedy například chceme určit všechny případy, kdy $\left(\frac{3}{p}\right) = 1$, tak dostáváme možnosti:

1. $(-1)^{\frac{p-1}{2}} = \left(\frac{p}{3}\right) = 1$, tedy $p \equiv 1 \pmod 4$ a $p \equiv 1 \pmod 3$. Snadno nahlédneme, že to splňují právě všechna prvočísla $p \equiv 1 \pmod{12}$.

2. $(-1)^{\frac{p-1}{2}} = \left(\frac{p}{3}\right) = -1$, tedy $p \equiv 3 \pmod 4$ a $p \equiv 2 \pmod 3$. Výpočtem získáme, že tohle splňuje právě zbytek $p \equiv 11 \pmod{12}$.

Podobně bychom mohli ověřit, že zbylé dvě možnosti $(-1)^{\frac{p-1}{2}} = -\left(\frac{p}{3}\right)$, pro které vyjde $\left(\frac{3}{p}\right) = -1$, přísluší právě prvočíslům, která dávají zbytek $p \equiv 5, 7 \pmod{12}$.

Dohromady tak dostáváme

$$\left(\frac{3}{p}\right) = \begin{cases} \text{nedefinováno} & \text{pokud } p = 2, \\ 0 & \text{pokud } p = 3, \\ 1 & \text{pokud } p \equiv \pm 1 \pmod{12}, \\ -1 & \text{jinak (tj. pokud } p \equiv \pm 5 \pmod{12}). \end{cases}$$

[1] Uvědomte si, že kvadratickou reciprocitu jde ekvivalentně formulovat jako $\left(\frac{p}{q}\right) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}}\left(\frac{q}{p}\right)$. Pokud nevěříte, zkuste si obě strany rovnosti přenásobit $\left(\frac{q}{p}\right)$. Obecně lze nenulové Legendreovy symboly v rovnostech „přehazovat ze strany na stranu“.