Teorie čísel: Cvičení 11 – výsledky, nápovědy, vzorová řešení

Simona Hlavinková, email: simonkahlavinkova@gmail.com

Nápovědy:

-1. Používejte standardní algoritmus předvedený na cvičení: Místo rozkladů na prvočinitele používejte hlavně vlastnosti (ii) a (iv), tedy periodicitu a kvadratickou reciprocitu. Multiplikativitou se zbavujte jen záporných nebo sudých argumentů.

0. V postupu se hned na dvou místech využije Čínská zbytková věta. Jacobiho symboly nehrají žádnou roli.

1. Jako v příkladu -1. Doporučuju nebát se záporných čísel!

2. (a) Stačí Legendreův symbol (který se dá spočítat pomocí nového algoritmu, neboť splývá s Jacobiho symbolem).
   (b) Legendreovy symboly mohou rozhodnout o existenci či neexistenci řešení, ale pokud řešení existuje, je nutné využít ČZV a explicitní kvadratické zbytky. Bez Legendreova/Jacobiho symbolu se zde lze bez problému obejít.
   (c) Opět použijte ČZV. Jacobiho symbol si spočítejte jen pro zajímavost.

3. Já jsem vám ty vztahy pro -1 a 2 už vtloukal do hlavy; teď si je můžete ověřit. Vztah pro -2 dostanete pochopitelně díky multiplikativitě.

4. (a) Vlastnost platí pro rozklad na jakákoliv po dvou nesoudělná čísla, ne nutně prvočísla. Jedna implikace je zjevná. Pro druhou si řešení jednotlivých kongruencí označte jako $x_1, \ldots, x_k$, sestavte si vhodnou soustavu kongruencí a použijte ČZV.
   (b) Odvoďte, že alespoň jedna z příslušných kongruencí nemá řešení.
   (c) Platí $(-1)^2 = 1$. :-)

5. Vyjděte přímo z definic (a vlastností Legendreova symbolu). Některé části jsou poněkud otravné, ale je to velmi přímočaré. U doplňků k reciprocitě doporučuju využít explicitních formulací z úlohy 3., tj. vztahů vycházejících z hodnot n modulo 4, resp. 8. (Možná jde nějak chytře odvodit přímo uvedený vzorec; já ale nevím, jak.)

6. Tuhle úlohu nedělejte, na testy prvočíselnosti bude samostatné cvičení. Zařadil jsem ji jen jako ilustraci použití Jacobiho symbolu a té jedné významné vlastnosti, kterou s Legendreovým symbolem nesdílí.

7. Ve všech případech předpokládejme, že $p_1, \ldots, p_n$ jsou všechna prvočísla požadovaného tvaru (v části a) jde o všechna prvočísla, v části b) i) prvočísla tvaru $4k + 3$ atd.).
   (a) Uvažujte číslo $p_1 \cdots p_n + 1$ nebo $m! + 1$, kde m je větší než všechna prvočísla. Co víte o jeho prvočíselných dělitelích?
   (b) Sestavte číslo tvaru $4k + 3$, resp. $6k + 5$ nesoudělné se všemi p_i. Co víme o jeho prvočíselných dělitelích?
   (c) Nehledám žádnou složitou odpověď, jen se zamyslete, kde se klíčový argument z předchozí části úlohy dá přímočaře použít a kde ne.
   (d) Použijte kvadratické zbytky.
   (e) Opět sestavte číslo vhodného tvaru, které bude nesoudělné se všemi danými prvočísly p_i.

Výsledky:

-1. -1.

0. $x \equiv 19, 30, 47, 58 \pmod{77}$. Ekvivalentně $x \equiv \pm 19, \pm 30 \pmod{77}$.

1. Samé -1. (Zvláštní náhoda.)

2. (a) První kongruence řešení má, druhá ne.
   (b) $x \equiv 39, 94, 115, 170 \pmod{209}$ neboli $x \equiv \pm 39, \pm 94 \pmod{209}$.
   (c) Kongruence nemá řešení (ačkoliv Jacobiho symbol vyjde 1).

3. - $\left(\frac{-1}{n}\right)$ je 1 pro $n \equiv 1 \pmod 4$ a -1 pro $n \equiv -1 \pmod 4$.
   - $\left(\frac{2}{n}\right)$ je 1 pro $n \equiv \pm 1 \pmod 8$ a -1 pro $n \equiv \pm 3 \pmod 8$.
   - $\left(\frac{-2}{n}\right)$ je 1 pro $n \equiv 1, 3 \pmod 8$ a -1 pro $n \equiv -1, -3 \pmod 8$.

4. (a) Tvrzení platí.
   (b) Tvrzení platí: Součin Legendreových symbolů je -1, takže alespoň jeden z nich je -1, tudíž příslušná kongruence nemá řešení. Díky jednodušší implikaci z bodu a) tudíž nemá řešení ani celá kongruence $x^2 \equiv a \pmod n$, neboli a není kvadratický zbytek modulo n.
   (c) Například $\left(\frac{58}{65}\right)$ z úlohy 2c) nebo $\left(\frac{2}{3\cdot 5}\right)$.

9. (a) $a^2 - ab + b^2$.
   (b) Tvrzení platí. (Existuje např. pěkný geometrický důkaz využívající toho, že tento okruh tvoří v rovině trojúhelníkovou síť a každý bod v rovnostranném trojúhelníku o straně 1 je k některému z vrcholů blíž než 1. Viz analogický důkaz se čtverci pro $\mathbb{Z}[\mathrm{i}]$.)
   (c) 3 a prvočísla tvaru $3k + 1$.
   (d) 3 a prvočísla tvaru $3k + 1$.

Vybraná vzorová řešení:
-1.) Budeme postupně používat vlastnosti Jacobiho symbolů, viz věta 4.14 ze skript.

$$\left(\frac{477}{247}\right) = \left(\frac{230}{247}\right) = \left(\frac{2}{247}\right)\left(\frac{115}{247}\right) = (-1)^{\frac{247^2-1}{8}}(-1)^{\frac{247-1}{2}\frac{115-1}{2}}\left(\frac{247}{115}\right) = -\left(\frac{17}{115}\right) =$$

$$= -(-1)^{\frac{115-1}{2}\frac{17-1}{2}}\left(\frac{115}{17}\right) = -\left(\frac{13}{17}\right) = -(-1)^{\frac{13-1}{2}\frac{17-1}{2}}\left(\frac{17}{13}\right) = -\left(\frac{4}{13}\right) = -\left(\frac{2}{13}\right)\left(\frac{2}{13}\right) = -1.$$

Všimněte si, že jsme se při výpočtu úplně vyhnuli rozkladu na prvočísla (kromě dělitelnosti 2).

Při vyčíslování výrazu $(-1)^{\frac{247^2-1}{8}}$ rozhodně nepočítáme druhou mocninu! Místo toho jen určíme, že $247 \equiv -1 \pmod 8$, takže hodnota je $+1$ (viz řešení příkladu 3.). Podobně při používání kvadratické reciprocity pouze ověřujeme, jestli je alespoň jedno číslo kongruentní 1 modulo 4, viz tamtéž. Alternativní způsob zápisu celého postupu viz řešení příkladu 1.

Ještě poznamenejme, že o něco efektivnější by bylo využívat i záporná čísla; takový výpočet by začínal $\left(\frac{477}{247}\right) = \left(\frac{-17}{247}\right) = \left(\frac{-1}{247}\right)\left(\frac{17}{247}\right) = \cdots$.

0.) Díky Čínské zbytkové větě je zadaný problém ekvivalentní s dvojící podmínek $x^2 \equiv 9 \pmod{11}$ a $x^2 \equiv 4 \pmod 7$. Snadno ověříme, že obě tyto kongruence už mají řešení. První z nich konkrétně $x \equiv \pm 3 \pmod{11}$ a druhá z nich $x \equiv \pm 2 \pmod 7$. Nyní už jen potřebujeme zpětně najít odpovídající zbytky modulo 77.

1. $x \equiv 3 \pmod{11}$ a $x \equiv 2 \pmod 7$. To odpovídá prvkům $x \equiv 58 \pmod{77}$.
2. $x \equiv 3 \pmod{11}$ a $x \equiv -2 \pmod 7$. To odpovídá prvkům $x \equiv 47 \pmod{77}$.
3. $x \equiv -3 \pmod{11}$ a $x \equiv 2 \pmod 7$. To odpovídá prvkům $x \equiv 30 \pmod{77}$.
4. $x \equiv -3 \pmod{11}$ a $x \equiv -2 \pmod 7$. To odpovídá prvkům $x \equiv 19 \pmod{77}$.

Řešením tedy jsou $x \equiv 19, 30, 47, 58 \pmod{77}$.

(Řešení 30 a 19 jsme mohli najít už z předchozích znalostí jako -47 a -58.)

1.) (a) Nezajímá nás, jde-li o Legendreovy symboly, nebo jestli je ve jmenovateli složené číslo a jde tudíž o Jacobiho, ale ne Legendreův symbol. Počítáme standardním postupem:

$$\left(\frac{98}{51}\right) = \left(\frac{-4}{51}\right) = \left(\frac{-1}{51}\right)\left(\frac{4}{51}\right) = -1 \cdot 1.$$

Poslední rovnost platí proto, že 51 je kongruentní 3 modulo 4, a protože 4 je kvadratický zbytek modulo všechno. (Alternativně se také dá psát $\left(\frac{4}{51}\right) = \left(\frac{2}{51}\right)^2$, a protože 2 je nesoudělné s 51, je v závorce ± 1 a ne nula, takže druhou mocninou je $+1$.)

(b) Podobně počítáme i jinde:

$$\left(\frac{89}{63}\right) = \left(\frac{26}{63}\right) = \left(\frac{2}{63}\right)\left(\frac{13}{63}\right) \overset{\text{A}}{=} \left(\frac{63}{13}\right) = \left(\frac{11}{13}\right) \overset{\text{B}}{=} \left(\frac{13}{11}\right) = \left(\frac{2}{11}\right) = -1,$$

přičemž rovnost A platí díky tomu, že $63 \equiv -1 \pmod 8$ a $13 \equiv 1 \pmod 4$; rovnost B díky tomu, že $13 \equiv 1 \pmod 4$; poslední rovnost pak proto, že $11 \equiv 3 \pmod 8$.

(c) Postup je stále stejný:

$$\left(\frac{347}{221}\right) = \left(\frac{-95}{221}\right) = \left(\frac{-1}{221}\right)\left(\frac{95}{221}\right) \overset{\text{A}}{=} \left(\frac{221}{95}\right) = \left(\frac{31}{95}\right) \overset{\text{B}}{=} -\left(\frac{95}{31}\right) = -\left(\frac{2}{31}\right) = -1;$$

rovnost A platí díky tomu, že $221 \equiv 1 \pmod 4$; rovnost B díky tomu, že $95 \equiv 31 \equiv -1 \pmod 4$; poslední rovnost pak proto, že $31 \equiv -1 \pmod 8$.

(d)

$$\left(\frac{675}{223}\right) = \left(\frac{6}{223}\right) = \left(\frac{2}{223}\right)\left(\frac{3}{223}\right) \overset{\text{A}}{=} (+1)(-1)\left(\frac{223}{3}\right) = -\left(\frac{1}{3}\right) = -1;$$

přitom rovnost A plyne z $223 \equiv -1 \pmod 8$, což dává i $223 \equiv -1 \pmod 4$. Poslední rovnost máme přímo z definice, protože 1 je kvadratický zbytek modulo cokoliv.

2.) (a) Úloha se nás ptá, zda jsou 18, resp. 14 kvadratické zbytky modulo 127. Protože je 127 prvočíslo, stačí vždy určit příslušný Legendreův symbol. Při jeho výpočtu můžeme „cestou“ použít i Jacobiho symboly, což vede k efektivnějšímu algoritmu (i když v tomto případě žádný takový krok provádět nebudeme):

$$\left(\frac{18}{127}\right) = \left(\frac{2}{127}\right)\left(\frac{9}{127}\right) = +1,$$

protože $127 \equiv -1 \pmod 8$ a protože 9 je kvadratický zbytek modulo cokoliv. Vyšlo $\left(\frac{18}{127}\right) = 1$, takže 18 je kvadratický zbytek modulo 127, neboli první z kongruencí má řešení.

$$\left(\frac{14}{127}\right) = \left(\frac{2}{127}\right)\left(\frac{7}{127}\right) = (+1)(-1)\left(\frac{127}{7}\right) = -\left(\frac{1}{7}\right) = -1,$$

kde jsme na vhodných místech využili toho, že $127 \equiv -1 \pmod 8$, že $127 \equiv 7 \equiv -1 \pmod 4$, a že 1 je kvadratický zbytek modulo cokoliv. Vyšlo $\left(\frac{14}{127}\right) = -1$, takže 14 není kvadratický zbytek modulo 127, neboli druhá z kongruencí nemá řešení.

(b) Rozmyslíme si, že pro každé $x \in \mathbb{Z}$ platí následující ekvivalence:

$$\begin{aligned} x^2 \equiv 58 \pmod{209} \quad &\iff \quad x^2 \equiv 58 \pmod{11} \quad \text{a} \quad x^2 \equiv 58 \pmod{19} \\ &\iff \quad x^2 \equiv 3 \pmod{11} \quad \text{a} \quad x^2 \equiv 1 \pmod{19} \\ &\iff \quad x \equiv \pm 5 \pmod{11} \quad \text{a} \quad x \equiv \pm 1 \pmod{19} \end{aligned}$$

První ekvivalence je Čínská zbytková věta, druhá je zjevná a třetí plyne z toho, že modulo prvočíslo má každá kongruence tvaru $x^2 \equiv a$ nejvýše dvě řešení.

Nyní už zbývá jen přepsat poslední podmínku díky ČZV zpátky do podoby jedné kongruence modulo 209. Jde o řešení čtyř soustav kongruencí:

Hledejme například řešení (díky ČZV existující a jednoznačné) soustavy $x \equiv 5 \pmod{11}$, $x \equiv 1 \pmod{19}$. Budeme procházet čísla tvaru $19k + 1$, dokud nenarazíme na některé, jehož zbytek modulo 11 je právě 5: $1, 20, 39, 58, 77, 96, 115$. Vidíme, že $x \equiv 115 \pmod{209}$ je řešením této soustavy.

Z toho okamžitě plyne, že -115 neboli 94 je řešením soustavy $x \equiv -5 \pmod{11}$, $x \equiv -1 \pmod{19}$. Řešení zbylých dvou soustav nalezneme analogicky (a samozřejmě existují i jiné metody, jak takovéto soustavy řešit).

Ve výsledku zjišťujeme, že řešením kongruence je $x \equiv \pm 39, \pm 94 \pmod{209}$, neboli $x \equiv 39, 94, 115, 170$. (Poznámka: Úloha to po nás nechtěla, ale kdybychom spočítali Jacobiho symbol $\left(\frac{58}{209}\right)$, vyšlo by nám $+1$. Dá se ukázat, že to je nutná, ale nikoliv postačující podmínka pro řešitelnost uvedené kongruence.)

(c) Uvedená kongruence je (díky ČZV) ekvivalentní dvojici kongruencí $x^2 \equiv 58 \pmod{5}$ a $x^2 \equiv 58 \pmod{13}$. Ptáme se tedy, je-li 58 zároveň kvadratickým zbytkem modulo 5 i modulo 13. Obě tyto otázky může rozhodnout Legendreův symbol (při jehož výpočtu se dají využít i Jacobiho symboly). Máme $\left(\frac{58}{5}\right) = \left(\frac{3}{5}\right) = -1$, protože 3 není kvadratický zbytek modulo 5. Z toho plyne, že nemůže být řešitelná ani původní kongruence, což je řešení příkladu.

Tento příklad ovšem ilustruje důležitý jev: Platí $\left(\frac{58}{65}\right) = +1$. Z toho vidíme, že to, že je Jacobiho symbol roven $+1$, ještě nezaručuje řešitelnost příslušné kongruence. (Důvodem je, že z definice platí $\left(\frac{58}{65}\right) = \left(\frac{58}{5}\right)\left(\frac{58}{13}\right)$, a oba výrazy vpravo jsou rovny -1, takže jejich součin je $+1$; aby ale byla kongruence řešitelná, potřebovali bychom, aby každý z nich byl roven 1 nebo 0.)