Errata bakalářské práce

Polynomiální a exponenciální kongruence

Matěj Kovářík

Titulní strana

Chybně vyplněn studijní program a obor. Správně:

Studijní program: Matematika se zaměřením na vzdělávání

Studijní obor: Matematika se zaměřením na vzdělávání se sdruženým studiem Anglický jazyk se zaměřením na vzdělávání

Str. 22

V tvrzení 4 nikde nefiguruje a, takže se zde podmínka $a \in \mathbb{Z}$ nemá vyskytovat.

Str. 23

V popisku obr. 1:

Chybně: Plné kolečko značí $\left(\frac{2}{p}\right) = -1$, prázdné $\left(\frac{2}{p}\right)$.

Správně: Plné kolečko značí $\left(\frac{2}{p}\right) = 1$, prázdné $\left(\frac{2}{p}\right) = -1$.

Str. 26

Záměna termínů *asymetrie* a *antisymetrie* v textu a popisku obr. 3 a 4.

Chybně: Nahlédněme do dvou obrázků, ve kterých jsme znázornili pouze symetrické a pouze asymetrické hodnoty.

Správně: Nahlédněme do dvou obrázků, ve kterých jsme znázornili pouze symetrické a pouze antisymetrické hodnoty.

Chybně: Schémata hodnot pro symetrické a asymetrické hodnoty $\left(\frac{p}{q}\right)$ a $\left(\frac{q}{p}\right)$.

Správně: Schémata hodnot pro symetrické a antisymetrické hodnoty $\left(\frac{p}{q}\right)$ a $\left(\frac{q}{p}\right)$.

Str. 34

Chybně: $\left[\frac{3}{3}\right] = 3$.

Správně: $\left[\frac{3}{3}\right] = 1$.

Str. 35

V závěru důkazu tvrzení 7 má být $(\mathrm{mod}\ p^2)$ namísto $(\mathrm{mod}\ p)$.

Str. 45

Příklad 19 je vyřešen chybně. Správné řešení:

Příklad 19: Vyřešte kongruenci $x^2 \equiv 100 \pmod{256}$.

Řešení: Použijme substituci $x = 2k$:

$$\begin{aligned} 4k^2 &\equiv 100 \ /:4 \\ k^2 &\equiv 25 \pmod{64} \end{aligned}$$

Dvěma očividnými řešeními jsou $k \equiv \pm 5$, ekvivalentně $k = 5 + 64l$ a $k = 59 + 64l, l \in \mathbb{Z}$. Zbylá dvě řešení nalezneme z jednoho ze zbylých tří řešení kongruence $k^2 \equiv 1 \pmod{8}$, tedy $k = 1, 3, 7 + 8m, m \in \mathbb{Z}$. K řešení vede jen $k = 3 + 8m$:

$$\begin{aligned} (3 + 8m)^2 &\equiv 25 \pmod{64} \\ 9 + 48m + 64m^2 &\equiv 25 \\ 48m &\equiv 16 \\ 16m &\equiv -16 \ /:16 \\ m &\equiv -1 \pmod{4} \\ m &\equiv 3 \end{aligned}$$

Druhou dvojicí řešení je tedy $k = 27 + 64l$ a $k = 37 + 64l$. Dosazením všech vyhovujících k máme řešení původní kongruence:

$$x \equiv 10, 54, 74, 118, 138, 182, 202, 246 \pmod{256}$$

Str. 47

Formulace závěru kapitoly je vzhledem k chybnému řešení příkladu 19 nepřesná. Konkrétně:

Chybně: Z příkladů je zřejmé, že takové kongruence budou mít čtyři řešení, namísto obvyklých dvou.

Správně: Z příkladu 20 a mezikroku řešení příkladu 19 je zřejmé, že kongruence $x^2 \equiv a \pmod{2^k}$ pro lichá a budou mít čtyři řešení, namísto obvyklých dvou.

Str. 49

Definice 6 má být značena Definice 7 a číslované je nadále posunuto v celé práci.

V úplném závěru důkazu tvrzení 11 je chybný index:

Chybně: $l_1 \cdot l_2 \cdot \ldots \cdot l_2$.

Správně: $l_1 \cdot l_2 \cdot \ldots \cdot l_m$.

Kap. 2 a str. 90

Posunuté číslování odkazování na tabulky. Odkaz na tab. č. n má být odkaz na tab. č. $n - 1$.

Str. 112

Chybně: $\mathbb{Z}_{16}^* \cong \mathbb{Z}_8$

Správně: $\mathbb{Z}_{16}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_4$