

str. 20, důkaz Eulerovy věty. Má být $c \equiv a^{\varphi(n)} \cdot c \pmod{m}$, nikoliv $=$.

str. 44, Obrázek 12. Podíl je spočítán špatně, správně mělo být $(-1 + 2i)/(3 + i) = -1/2 + 1/2i$.

str. 80 nahoře. $m \times (a * b) = (m \times a) * (m \times b)$ samozřejmě platí pouze v abelovských grupách.

str. 80, konec důkazu Tvrzení 14.3. Má být $((k_1 \times x_1) * \dots * (k_n \times x_n))' = (-k_n \times x_n) * \dots * (-k_1 \times x_1)$.

str. 83, Tvrzení 15.1. Důkaz je formulován poněkud nepořádně. Pořádný důkaz je například tento:

Důkaz. Podle Tvrzení 14.3. je $\langle a \rangle_{\mathbf{G}} = \{k \times a : k \in \mathbb{Z}\}$. Předně si všimněme, že $u \times a = v \times a$ právě tehdy, když $(u - v) \times a = e$. Pokud tedy žádné n s vlastností $n \times a = e$ neexistuje, uvedené prvky podgrupy $\langle a \rangle_{\mathbf{G}}$ jsou po dvou různé a tato podgrupa je nekonečná. Uvažujme nadále nejmenší kladné n takové, že $n \times a = e$. Pak

$$0 \times a, 1 \times a, \dots, (n - 1) \times a$$

jsou po dvou různé prvky podgrupy $\langle a \rangle_{\mathbf{G}}$, takže její velikost je aspoň n . Na druhou stranu, pro $q = k \operatorname{div} n$ a $r = k \bmod n$

$$k \times a = (qn + r) \times a = q \times (n \times a) * (r \times a) = (q \times e) * (r \times a) = r \times a,$$

takže podgrupa $\langle a \rangle_{\mathbf{G}}$ obsahuje přesně n prvků. □

str. 87, Věta 15.9 má daleko jednodušší a elegantnější důkaz, jak jsem zjistil:

Věta. *Bud' \mathbf{G} konečná podgrupa grupy \mathbf{T}^* , kde \mathbf{T} je nějaké těleso. Pak \mathbf{G} je cyklická.*

Lemma. *Bud' $\mathbf{G} = (G, *, ', e)$ konečná grupa a předpokládejme, že pro každé $k \in \mathbb{N}$ existuje nejvýše k prvků a splňujících $k \times a = e$. Pak \mathbf{G} je cyklická.*

Důkaz. Označme u_k počet prvků řádu k v grupě \mathbf{G} , položme $n = |G|$. Pokud $k \nmid n$, pak podle Tvrzení 15.2 je $u_k = 0$. Naopak, pokud $u_k \neq 0$, uvažujme nějaký prvek a řádu k . Pak $\langle a \rangle_{\mathbf{G}}$ je cyklická grupa řádu k , a tedy všechny prvky $b = u \times a$, $u = 0, \dots, k - 1$, splňují $k \times b = e$. Podle předpokladu jsme našli všechna řešení této rovnice, takže $\langle a \rangle_{\mathbf{G}}$ je jediná cyklická podgrupa řádu k v \mathbf{G} . Podle Věty 15.7 má $\varphi(k)$ generátorů, tedy $u_k = \varphi(k)$.

Shrnuto, pro každé $k \mid n$ platí $u_k = 0$ nebo $u_k = \varphi(k)$. Přitom $\sum_{k \mid n} u_k = n$, a zároveň podle úlohy pod Větou 15.7 je $\sum_{k \mid n} \varphi(k) = n$. Tedy $u_k = \varphi(k)$ pro všechna $k \mid n$, speciálně tedy v \mathbf{G} existuje prvek řádu n . □

Důkaz Věty. Je-li \mathbf{T} těleso, podle Věty 10.2 má polynom $x^k - 1$ nejvýše k kořenů v \mathbf{T} . Tedy v $\mathbf{G} \leq \mathbf{T}^*$ existuje nejvýše k prvků splňujících $a^k = 1$ a můžeme aplikovat předchozí lemma. □

str. 91, poslední odstavec o RSA. dvakrát překlep d vs. e (znalost d , způsob výpočtu d).

str. 124, poslední řádek. Ve skutečnosti dostaneme $\mathbb{Z}[x]/x^2 - 1 \simeq \text{Im}(\varphi)$, což ovšem není $\mathbb{Z} \times \mathbb{Z}$, nýbrž jeho podokruh tvořený prvky (a, b) takovými, že $a \equiv b \pmod{2}$.