Bohužel se mi písemka povedla těžší, než jsem chtěl; proto jsem nakonec trochu snížil počet bodů potřebných k získání zápočtu. Napíšu sem pár chybiček a podnětů k zamyšlení, co mě tak při opravování napadly.

Největší problémy byly se 3. a 4. příkladem.

3. příklad: Tady bych chtěl jen podotknout, že neplatí $o(ab) = \frac{o(a)o(b)}{NSD(o(a),o(b))}$ (pro obecné prvky a, b), jak by tak člověk naivně čekal (taky mi trvalo pěknou chvíli, než jsem si uvědomil, proč to nejde (:). Zvolíme-li ale třeba $b = a^{-1}$, bude $o(a) = o(b) = n$, takže $\frac{o(a)o(b)}{NSD(o(a),o(b))} = n \neq o(ab) = o(1) = 0$. V tomto příkladě na něco kloudného přišel jen Řezáč, který u mě má za odměnu čokoládu (:

4. příklad: V částech b) i c) se objevil stejný zádrhel, který ukazuje, proč je (aspoň někdy) potřeba neodbývat ověřování definice - v tomto případě homomorfismu. V $\mathbb{Z}_n$ se počítá tak, že $a \oplus b = (a + b \pmod n)$, kde $\oplus$ je grupová operace v $\mathbb{Z}_n$ (kterou jsem v zadání značil normálním +) a + je sčítání v celých číslech. Je tedy $\varphi(a \oplus b) = \varphi(a + b \pmod n) = i^{a+b \pmod n}$. Chceme-li ověřit, zda je φ homomorfismus, musíme tedy zjistit, jestli platí $i^{a+b \pmod n} = i^a i^b$. To zvládla jen Věra Šetmaňuková a má za to u mě čokoládu (:

V 6. příkladě někteří z vás bohužel zapomněli na to, že náhrdelník jde i překlopit; kupodivu bohužel nikdo nedokázal dojít ke správnému výsledku (nejčastěji byl problém právě v počtu pevných bodů překlopení).

7. příklad (který je trochu těžší, což jsem i - narozdíl od trojky - chtěl) nevyřešil nikdo. Občas se objevil jen následující špatný postup:

Podle Lagrangeovy věty musí řád každého prvku dělit velikost grupy. $p|p^k$, podmínka Lagrangeovy věty je splněna, a tedy takový prvek existuje.

To jsme ale nedokázali! Dokázali jsme, že existence daného prvku NEODPORUJE Lagrangeově větě, z toho ale nemůžem vyvodit, že prvek existuje. Co kdyby jeho existence odporovala něčemu jinému? Co kdyby prvek někdy existoval a někdy ne?