

Poučenie z krízového vývoja... ☺

- (a) Všetky číselné údaje v tomto texte sa týkajú len študentov FIIT. Pokiaľ ide o všeobecné komentáre a najčastejšie sa vyskytujúce problémy v riešeníach úloh, tak tie sa pravdepodobne týkajú rovnako aj študentov FEI.
- (b) Písomku písalo všetkých 55 zapísaných študentov.
- (c) Celkové výsledky písomky dopadli dobre. Priemerná úspešnosť bola približne 73.5%. Priemerné bodové výsledky a priemerná úspešnosť za jednotlivé úlohy sú uvedené v nasledovnej tabuľke

	1.	2.	3.	4.	5.	Spolu
Body	3.982	1.533	0.805	9.855	2.741	18.382
Úspešnosť	99.50 %	51.10 %	26.80 %	82.10 %	91.40 %	73.50 %

- (d) Plný počet bodov mala len **jediná** študentka – jej gratulujem a ostatní nech sa do ďalšej písomky zlepšia!!!
- (e) Ako vidno aj z vyššie uvedenej tabuľky, najlepšie dopadli úlohy 1 a 5. Len jediný študent nemal plný počet bodov za 1. úlohu a za 5. úlohu len zopár študentov stratilo body. Tieto dve úlohy boli čisto „počítacie“. Išlo teda len o naučenie sa algoritmu a následné „dosadzovanie do naučených vzorcov“. Toto zvládli všetci bez problémov. Problém je v tom, že toto zláadne aj cvičená opica, pretože to je činnosť nevyžadujúca takmer žiadne myslenie.
- (f) Najhoršie dopadla 3. úloha, čo bola úloha v podstate identická s úspešnou 5. úlohou, akurát namiesto čísel boli v Jacobiho symbole „písmená“ a pri riešení tejto úlohy bolo treba aj trochu myslieť a nielen mechanicky „dosadzovať do naučených vzorcov“. Takmer všetci študenti pravidlá na výpočet Jacobiho symbolu buď vedeli, alebo mali napísané na „ľaháku“ a pri riešení 5. úlohy aj preukázali, že ich vedia používať. Ale v 3. úlohe bolo treba pracovať s abstraktnými symbolmi (písmenami) namiesto čísel a väčšina študentov zlyhala! Len **traja** študenti mali za túto úlohu plný počet bodov a 0 bodových študentov bola väčšina.
- (g) Úloha 2 dopadla ako druhá najhoršia. Bodová úspešnosť bola tesne nadpolovičná. Opäť bol problém s abstraktným myslením. Ak by bola úloha formulovaná s konkrétnymi číslami, tak by zrejme takmer všetci vedeli zistiť, či daná afinná funkcia je permutáciou a mali by plný počet bodov. Ale v zadaní neboli čísla, lež $\alpha(x) = ax + b \pmod{27}$ a už mala väčšina študentov problém „čo s tými a a b “!
- (h) Úloha 4 dopadla dobre. Postup riešenia kvadratickej kongruencie ovládali takmer všetci študenti. Problémy sa vyskytli väčšinou vo forme numerických chýb a za tie bol strhávaný len symbolický počet bodov, pretože tie nie sú až také dôležité.
- (i) Poučenie z tejto písomky je také, že úlohy s konkrétnymi číselnými hodnotami študenti vedia riešiť bez problémov. Na takéto úlohy stačí poznať algoritmy ich riešenia a potom už len správne spočítať číselné hodnoty. Dokonca aj tak komplexný príklad ako bola 4. úloha, kde

bolo treba spraviť kánonický rozklad čísla, zostaviť sústavu kongruencií, nájsť odmocninu vo zvyškovej triede na základe Eulerovho kritéria a s pomocou squaring algoritmu, počítať multiplikatívne inverzné prvky pomocou rozšíreného Euklidovho algoritmu, zostaviť sústavy pre Čínsku zvyškovú vetu a vyriešiť ich, nerobilo väčšine študentov žiaden problém. Avšak pri jednoduchých a ďaleko menej komplexných úlohách, v ktorých sa namiesto konkrétnych číselných hodnôt vyskytli písmená a ktoré vyžadovali abstraktné myslenie a zovšeobecnenia, väčšina študentov zlyhala.

Toto je oblasť, v ktorej treba na sebe intenzívne pracovať. Abstraktné myslenie, dôkladná analýza a všeobecné riešenia problémov sú v matematike samozrejmosťou a rovnako dôležité sú aj pre informatikov. Dokázať, že $3 + 5$ ale $1 + 7$ sú párne čísla dokáže už prvák na základnej škole, pretože sa to dá spraviť konkrétnym výpočtom. Ale s pomocou abstrakcie a zovšeobecnenia sa dá ľahko dokázať, že súčet ľubovoľných dvoch nepárnych čísel je párne číslo. Podobne je to napríklad aj s Jacobiho symbolom z 3. a 5. úlohy. Vypočítať hodnotu Jacobiho symbolu pre konkrétne číselné hodnoty (5. úloha) a s pomocou vzorcov na jeho výpočet dokáže každý, kto ovláda základné aritmetické operácie a vie čítať a písať. Ale na výpočet Jacobiho symbolu $J\left(\frac{p^\alpha}{q^\beta}\right)$ z 3. úlohy je potrebné pravidlá na výpočet Jacobiho symbolu nielen poznať a vedieť ich mechanicky používať, ale je potrebné im aj rozumieť, t. j. poznať definíciu Jacobiho symbolu a vedieť z nej jednotlivé pravidlá odvodiť a dokázať. To už vyžaduje schopnosť abstraktného myslenia, ktoré budete potrebovať rovnako aj pri riešení informatických problémov v praxi (za predpokladu, že sa nebudete živiť len tvorbou webových stránok). Pri riešení problému musíte najskôr pochopiť jeho podstatu a pokiaľ to je možné, tak problém vyriešiť všeobecne. Ak budete problém riešiť len pre konkrétnu situáciu a konkrétne vstupné hodnoty, tak sa vám môže stať, že pri nepredvídaných vstupoch bude vaše riešenie zlé, alebo nebude fungovať vôbec. Záverom ešte jedna „bájka“ na túto tému

Do opevneného hradu sa chcel dostať nepriateľský špión. Hradnú bránu však strážili zbrojnoši a každému prichádzajúcemu povedali heslo, na ktoré musel tento odpovedať podľa dohodnutého kódu. Špión sa preto schoval v húštine neďaleko brány a sledoval dianie pri bráne

- ★ zbrojnoši: „štrnásť“ 1. prichádzajúci: „sedem“
- ★ zbrojnoši: „desať“ 2. prichádzajúci: „päť“
- ★ zbrojnoši: „osem“ 3. prichádzajúci: „štyri“

Následne sa špión sám vybral k bráne mysliac si, že už pozná dohodnutý kód. Zbrojnoši mu povedali heslo „šesť“ a on odpovedal „tri“, na čo sa naňho zbrojnoši vrhli a zabili ho.

Takže pozor na to, aby ste aj vy neriešili problémy podobne, len pre zopár konkrétnych hodnôt a nedopadli ako ten špión!

PS: Som zvedavý kto mi ako prvý pošle správnu odpoveď na heslo „šesť“ a samozrejme aj popis kódu. Pomôcka: pre heslo „šestnásť“ je odpoveď „osem“, ale pre heslo „osemnásť“ je takisto odpoveď „osem“.