Závěrečná zpráva projektu specifického výzkumu – zakázka č. 2111

Název projektu:

Determinanty speciálních třídiagonálních matic a kryptografie založená na eliptických křivkách

Odpovědný řešitel: RNDr. PaedDr. Pavel Trojovský, Ph. D.

Studenti magisterského studia na PdF UHK:

Eva Hladíková	*V/SSK*	*Ma – Vv*
Jana Pazderová	*IV/ZS2*	*Ma – Aj*
Jan Smejkal	*IV/ZS2*	*Ma – Aj*

Další výzkumní pracovníci: RNDr. Jitka Kühnová, Ph. D.

Celková částka přidělené dotace: 108 811 Kč

Stručný popis postupu při řešení projektu

Řešitelský kolektiv navázal při řešení uvedeného projektu v roce 2011 na svou předchozí práci v uvedené problematice, která byla zdokumentována ve výstupech řešení projektů specifického výzkumu v předchozích pěti letech.

Po odborné stránce jsme se při řešení projektu specifického výzkumu zaměřili především na zkoumání v problematice determinantů speciálních matic a především pak na tematiku třídiagonálních matic. Řešitelé se dále věnovali algebraickým metodám v kryptografii, speciálně však asymetrické kryptografii. Příslušné publikační výstupy jsou dále uvedeny.

Dále jsme se soustředili na průběžnou inovaci obsahu výběrových přednášek nabízených členy řešitelského kolektivu studentům vyšších ročníků. Členové řešitelského kolektivu se zapojili do seminářů organizovaných pro nadané středoškolské studenty.

Výsledky řešení projektu

1. Příspěvek na 20th Czech and Slovak International Conference on Number Theory (Stará Lesná 2011, Slovakia), P. Trojovský.
2. Příprava a korektury článků pro odborné časopisy (viz seznam publikací).
3. P. Trojovský je recenzentem recenzního časopisu *Mathematical Reviews* vydávaného American Mathematical Society, pro který recenzoval tři články v průběhu roku 2011.
4. Byl uspořádán seminář pro nadané středoškolské studenty.

Splnění kontrolovatelných výsledků řešení

V době řešení projektu již vyšel článek:

Trojovský, P., Hladíková, E. On the Hessian of the Exponential Function with ν Variables, Int. J. Pure Appl. Math., 2011, Vol. 66, No. 3, s. 287.295. ISSN 1311.8080
(**časopis je zařazen v databázi SCOPUS**)

V době řešení projektu byl přijat článek:

Trojovský, P., Seibert, J. On factorization of the Fibonacci and Lucas numbers using tridiagonal determinants. Mathematica Slovaca
(**časopis je zařazen v databázi WoS, jde o impaktovaný časopis**)

V recenzním řízení jsou články:

Kühnová, J., Pazderová, J., Smejkal, J. Eulerovo číslo a jeho výpočet pomocí číselných řad a řetězových zlomků, odesláno do Matematika-Fyzika-Informatika.

Trojovský, P., Hladíková, E. Symetrická kryptografie a standardy DES a AES, odesláno do Media4U.

Trojovský, P., Hladíková, E. Kryptografie založená na eliptických křivkách, odesláno do Media4U.

Přehled realizovaných výdajů:

a) osobní náklady

J. Kühnová	2000 Kč	Spolupráce na přípravě jednoho článku.
P. Trojovský	3000 Kč	Spolupracoval na jednom v letošním roce publikovaném článku v časopisu zařazeném ve SCOPUS, na dvou článcích odeslaných do časopisu v „Seznamu…ČR - 2011“, jednoho článku přijatého v impaktovaném časopisu Mathematica Slovaca. Přednáška na mezinárodní konferenci „20th Czech and Slovak Conference on Number Theory“ (Slovensko).
	1 721 Kč	odvody na zdravotní, sociální a úrazové pojištění atd.
Celkem	**6721 Kč**	

b) stipendia a jejich stručné zdůvodnění

Eva Hladíková	6000 Kč	Spolupráce na přípravě dvou článku, které jsou v recenzním řízení a jednoho článku, který vyšel v časopise zařazeném do databáze Scopus.
Jana Pazderová	3000 Kč	Spolupráce na přípravě jednoho článku a překlady odborných textů.
Jan Smejkal	3000 Kč	Spolupráce na přípravě jednoho článku a překlady odborných textů.
Celkem	**12000,40 Kč**	

c) materiálové náklady, služby (výdaje na pořízení drobného dlouhodobého hmotného majetku, nehmotného majetku – software, kancelářské potřeby, ostatní materiál) a jejich stručné zdůvodnění

Počítač s monitorem	24 561 Kč
Software Mathematica 8.0	27 245 Kč
Spotřební materiál	22 067,65 Kč
celkem	**73 873,65**

d) další náklady (služby, jiné výdaje) a jejich stručné zdůvodnění

Konferenční poplatek za 20th Czech and Slovak Conference on Number Theory	8 972,50 Kč
Přednáškový pobyt SAV Bratislava, cestovné	11 388 Kč
Celkem	**20 360,50 Kč**
Celkem a) b) c) d)	**112 955,55 Kč**

Veškeré přidělené finance na projekt byly tedy bohužel přečerpány o **4 144,55 Kč**, což je způsobeno nepřesným závěrečným dokoupením spotřebního materiálu.

Hradec Králové 2. ledna 2011

PaedDr. RNDr. P. Trojovský, Ph.D.
odpovědný řešitel