Pokroky matematiky, fyziky a astronomie

Otokar Grošek

O vzťahu akademika Štefana Schwarza k aplikáciám matematiky

Pokroky matematiky, fyziky a astronomie, Vol. 43 (1998), No. 4, 314--319

Persistent URL: http://dml.cz/dmlcz/139747

O vzťahu akademika Štefana Schwarza k aplikáciám matematiky

Otokar Grošek, Bratislava

Dovoľte mi podeliť sa o niekoľko osobných spomienok, ktoré sú iste poznačené „kapacitou mojej pamäti", nášho blízkeho vzťahu ako aj mojej osobnej interpretácie jeho slov a myšlienok. Ale bez ich vyslovenia by druhá — čisto odborná časť — nebola možno pochopená správne.

Poznal som ho od r. 1965. Mal som rád (okrem iných vecí) aj matematiku a on bol vždy prístupný na debaty o matematike a jej poslaní. Okrem „politiky" sme sa bavili o riešení príkladov MO všetkých kategórií, o výchove „závodných koňov" (rozumej sústredenia MO a MMO, kde sa preberala látka *navyše*).

Neskôr, keď som študoval na PF UK, dostali naše debaty nový rozmer. Často som nechápal, načo sa učíme niektoré partie. Na tabuli sa objavovali viac či menej brilantné dôkazy, ale mne chýbala motivácia mimo matematiky.

Priznávam, že jedným z cieľov našich debát o aplikáciách matematiky bolo odniesť si nejakú knihu či priamo jeho poznámky. Mojím prvým úlovkom boli tri diely *Matematika, jejo soderžanie, metody i značenie* napísaná pod vedením A. D. Alexandrova, A. N. Kolmogorova a M. A. Lavrentieva. V jeho zošite požičaných kníh je dodnes zápis: požičané Otovi na 99 rokov. Tak som sa ako čerstvý absolvent PF dozvedel, čo je to Fourierov rad, Cauchyho-Riemannove podmienky, i, komplexný logaritmus, Jakobián, atď. A pretože nasledujúce dve oblasti, v ktorých akademik pracoval, a ktorých výsledky majú značný význam pre prax, súvisia s počítačmi, dovoľte ešte jeden postreh: Dovolím si tvrdiť, že sa nikdy *nespriatelil* s počítačom ani len na úrovni textového editora. Hovorieval, že keď píše, tak rozmýšľa, a to sa s počítačom nedá! Všetky listy písal až do svojej smrti doma na drevenej doske pripevnené špendlíkmi a cez indigo... Niektoré boli potom samozrejme prepisované po jeho osobnej viacnásobnej korektúre.

Akademik vždy uprednostňoval termín „aplikácie matematiky" pred termínom „aplikovaná matematika". Hovorieval, že matematika je len jedna a nedá sa deliť. Sám nikdy nenapísal prácu, v ktorej by bol explicitne uvedený nejaký aplikačný výstup, resp. riešený konkrétny problém z „praxe". Je to skutočne neuveriteľné, lebo každý, kto mal to šťastie a počúval jeho prednášky, vie, že boli poprepletané množstvom príkladov z fyziky či elektrotechniky! Všetky poznámky a prípravy na prednášky si starostlivo archivoval.

Pamätám sa, že jedna z našich tém boli dva významné objavy, v pozadí ktorých bola matematika (vždy sa to nejako prepletalo s históriou):

Prof. RNDr. Otokar Grošek, CSc. (1950), katedra matematiky Fakulty elektrotechniky a informatiky Slovenskej technickej univerzity, 812 19 Bratislava, SR. E-mail: GROSEK@kmat.elf.stuba.sk

1. *Mendelejev vymyslel v r. 1869 tabuľku, v ktorej podľa istých kritérií usporiadal chemické prvky. Vznikli mu prázdne okienka, a pretože svojmu objavu veril, zákonite predpokladal, že v budúcnosti zaplnia tri prázdne miesta v štvrtej perióde dovtedy neznáme prvky. Tak sa postupne stalo, že v období 1875–1886 bolo objavené gallium, germanium a scandium.*

názov	chem. značka	atóm. číslo	objaviteľ	krajina	rok
gallium	Ga	31	Paul de Boisbaudran	Francúzsko	1875
germanium	Ge	32	Clemens Winkler	Nemecko	1886
scandium	Sc	21	Lars Nilson	Švédsko	1879

2. *Planéta Neptun bola najprv vyrátaná a až potom „videná“*[1]) *na oblohe. Astronómovia pozorovali, že Urán považovaný za najvzdialenejšiu planétu našej slnečnej sústavy sa nenachádzal vždy tam, kde predpokladali. To znamená, že gravitačné sily neznámej planéty pôsobia na Urán. Tieto výpočty ako prvý vykonal mladý anglický matematik a astronóm J. C. Adams*[2]) *v r. 1843, ale nikto zo zodpovedných mu neveril. Až keď k rovnakému výsledku dospel v r. 1846 francúzsky matematik J. J. Leverrier a nemecký astronóm J. G. Galle našiel planétu presne tam, kde podľa výpočtov mala byť, svet uveril...*

JE MOŽNÝ TAKÝTO OBJAV V SAMOTNEJ MATEMATIKE?

Odpoveď nie je jednoduchá, lebo nie je jednoduché definovať „objav“ v matematike. Napríklad Fermat predpokladal, že čísla tvaru

$$F_m = 2^{2^m} + 1, \quad m = 0, 1, 2, \ldots,$$

sú prvočísla. Už Euler dokázal, že F_5 nie je prvočíslo (našiel jeho faktor 641). Podľa tzv. Pepinovho kritéria F_m je prvočíslo práve vtedy, ak

$$3^{(F_m-1)/2} \equiv -1 \pmod{F_m}. \tag{1}$$

Takto je možné dokázať, že F_{14}, F_{20} a F_{22} sú zložené, hoci nepoznáme žiadne ich faktory[3]). Bude to objav, ak niekto nájde tieto faktory?

Ale aplikácie matematiky veľmi často „asistujú“ pri objavoch v iných vedách, dokonca veľmi často sú ich nevyhnutným predpokladom.

A teraz už nastal čas, aby sme na konkrétnych príkladoch dokázali, že akademik Š. Schwarz minimálne v dvoch prípadoch dokázal výsledky, ktoré mali priame aplikácie v technickej praxi.

---

[1]) Je to jedna z dvoch planét, ktoré nemožno vidieť bez použitia dobrého teleskopu. Jej prvé fotografie „zblízka“ boli získané až v r. 1989 prostredníctvom sondy Voyager 2.

[2]) Bol to ten istý Adams, ktorý vyrátal prvých 62 Bernoulliho čísel a odhalil viacero ich vlastností.

[3]) Uvážte, že číslo F_m má $0{,}301 \cdot 2^m$ desiatkových cifier. Pre $m = 14$ je to 4933 cifier.

Problém prvý. Už 10. marca 1938 mal mladý Schwarz prednášku v Matematickom ústave Prírodovedeckej fakulty KU v Prahe s názvom *O irreducibilitě polynomů.* V nasledujúcich 8–10 rokoch o tejto problematike uverejnil niekoľko článkov. Samozrejme, kto v tom čase uvažoval o ich uplatnení pri kódovaní správ, či utajovaní informácií?!

Bez faktorizácie polynómov nad konečným poľom sa v týchto disciplínach vôbec nepohneme. Napríklad taký vzorec, udávajúci počet irreducibilných polynómov nad GF(2) stupňa k, ktoré delia polynóm $D^N - 1$ pre N nepárne[4]):

$$\sigma_k = \frac{1}{k} \sum_{t|k} \mu\left(\frac{k}{t}\right) \mathrm{GCD}(N, 2^t - 1), \tag{2}$$

kde μ je tzv. Möbiusova funkcia, t.j.

$$\mu(n) = \begin{cases} 1; & \text{ak } n = 1, \\ 0; & \text{ak } u^2 \mid n \text{ pre nejaké prvočíslo } u, \\ (-1)^k; & \text{ak } n \text{ je súčinom presne } k \text{ rôznych prvočísel.} \end{cases} \tag{3}$$

Jeho význam, napr. pri hľadaní kódov, si môžeme ilustrovať na nasledujúcom probléme. Platí [3]:

Veta. *Ľubovoľný cyklický kód s L informačnými znakmi a dĺžkou slova N je generovaný polynómom $g(D)$ stupňa $N - L$. Takýto polynóm delí $D^N - 1$. Naopak, ľubovoľný polynóm stupňa $k = N - L$, ktorý je deliteľom $D^N - 1$, generuje nejaký cyklický kód s L informačnými znakmi a dĺžkou kódoveho slova N.*

Vzorec (2) vlastne hovorí, že ak $\sigma_k = 0$, tak taký polynóm neexistuje. Naopak, ak $\sigma_k \neq 0$, tak má zmysel ho hľadať. (Biele miesto v tabuľke Mendelejeva, či neznáma planéta?)

Problém druhý. V roku 1943 — nesmierne ťažkom období pre neho samotného — v takmer úplnej izolácii publikoval svoju habilitačnú prácu [4] *Teória pologrúp.* V nej okrem iného študoval maximálne grupy v periodických pologrupách. Uveďme dve vety z tejto pionierskej práce (bez jazykovej úpravy)[5]):

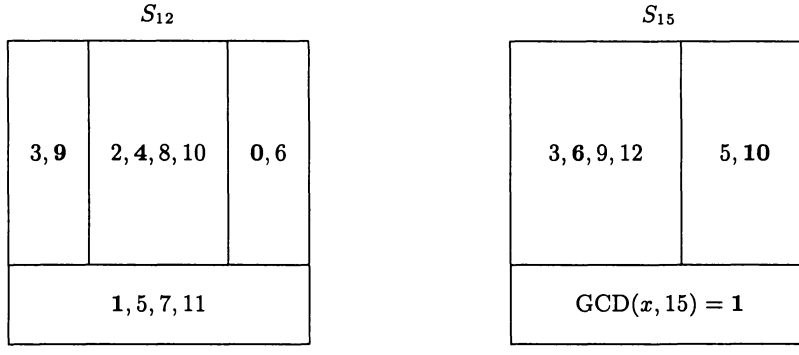
Veta 6. *Nech je $\mathfrak{M}$ pologrupou, ktorej každý element je konečného radu. Ku každému idempotentu e pologrupy $\mathfrak{M}$ jestvuje jedna a len jedna maximálna grupa, ktorá má e za jednotkový element. Dve maximálne grupy, ktoré prislušia ku dvom rôznym idempotentom, nemajú spoločného elementu.*

Veta 7. *Nech je $\mathfrak{M}$ pologrupou, ktorej každý element je konečného radu. Nevyhnutná a postačujúca podmienka pre to, aby $\mathfrak{M}$ bolo súčtom svojich maximálnych grúp je, aby žiadny element z $\mathfrak{M}$ neobsahoval predperiódu.*

Na obrázkoch sú znázornené takéto rozklady multiplikatívnych pologrúp $S_m = \{0, 1, 2, \ldots, m-1\}$ s operáciou $*$ (mod m) pre $m = 12$ resp. 15. Tučne sú vyznačené

[4]) Vzorec mlčky predpokladá, že poznáme faktorizáciu k.

[5]) Idempotent e pologrupy S je taký prvok, pre ktorý platí $e^2 = e$.



Obr. 1. Rozklady multiplikatívnych pologrúp S_{12} a S_{15}.

idempotenty. Množina $\{2, 4, 8, 10\}$ je len podpologrupa. Prvok 2 totiž obsahuje predperiódu:

$$2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 8, \quad 2^4 \equiv 4, \quad \ldots$$

Príslušná maximálna grupa je v tomto prípade $G(4) = \{4, 8\}$. Vagner [8] zovšeobecnil tieto výsledky na ľubovoľné pologrupy a zaviedol pojem zovšeobecnenej inverzie, ktorý Thierrin [7] nazýva *reciprocal.*

Pologrupa S sa nazýva *regulárna*, ak pre každé $a \in S$ existuje aspoň jedno riešenie rovnice $axa = a$, $x \in S$. Poznamenajme, že v takom prípade sú $e = ax$ aj $f = xa$ idempotenty, pre ktoré platí $ea = af = a$. Pologrupa S_{12} regulárna nie je, lebo rovnica $2 * x * 2 \equiv 2 \pmod{12}$ nemá riešenie. Pologrupa S_{15} regulárna je.

Prvá aplikácia

V r. 1965 publikoval Schwarz článok [5], kde s pomocou aparátu teórie pologrúp dokázal tri základné výsledky známe z ergodickej teórie stochastických matíc (Markovovských reťazcov). Išlo vlastne o rozklad pologrupy $\mathfrak{S}_n$ všetkých $n \times n$ stochastických matíc na maximálne grupy.

Veta. [5] *Nech* $\mathbf{P} \in \mathfrak{S}_n$ *patrí k pozitívnemu primitívnemu idempotentu* $\mathbf{U}$. *Potom nutná a postačujúca podmienka na to, aby postupnosť* $\mathbf{P}, \mathbf{P}^2, \mathbf{P}^3, \ldots$ *konvergovala, je splnenie podmienky* $\mathbf{PU} = \mathbf{UP} = \mathbf{U}$. *Navyše potom platí* $\lim_{k \to \infty} \mathbf{P}^k = \mathbf{U}$.

Tieto výsledky viedli k veľmi prirodzenej otázke, ktorú akademik Schwarz položil: popísať všetky matice zo $\mathfrak{S}_n$ patriace ku danému primitívnemu idempotentu. Tento problém sa prirodzene vyskytol o 15 rokov neskôr pri štúdiu stochastických automatov.

Praktický problém spočíval v nasledovnom: Pozorujeme markovský zdroj správ, ktorý je ergodický a regulárny. Zmena stavov je však taká rýchla, že sme schopní zmerať len relatívnu frekvenciu výskytu jednotlivých stavov a nie relatívnu frekvenciu prechodov. V reči matematiky: je známy len primitívny idempotent, ku ktorému patrí pozorovaná prechodová matica. Úlohou je nájsť všetky (potenciálne) možné matice, patriace k danému idempotentu. Riešenie je uvedené v [2].

Druhá aplikácia

Typickým príkladom periodickej pologrupy je už spomínaná pologrupa S_m s násobením $*\pmod m$. Špeciálnym prípadom je $m = pq$, kde p a q sú rôzne nepárne prvočísla, kedy je táto pologrupa aj regulárna. Samozrejme, všetky Schwarzove výsledky z r. 1943 platia aj pre tento špeciálny prípad. Navyše, v r. 1981 (len 3 roky po publikovaní RSA-algoritmu, ktorý funguje práve vďaka regulárnosti S_m) napísal prácu [6]. Obsahom práce je prehľad známych výsledkov o pologrupe S_m, ako aj nové vzorce pre počet riešení kongruencie[6])

$$x^d \equiv x^k \pmod m. \tag{4}$$

Keď písal tento článok, netušil možné použitie týchto výsledkov v kryptológii. Zato v **MR** 83b: 10015 je možné nájsť takmer dvojstĺpcovú recenziu pochádzajúcu od L. Kuipersa. Samozrejme čitatelia MR vedia, že takéto obsiahle recenzie sa vyskytujú veľmi zriedkavo. S pomocou týchto výsledkov sa napríklad podarilo opísať taký výber vhodných prvočísel p, q, pre ktoré je tzv. *iterovaný útok* najmenej úspešný [1].

Známy RSA-algoritmus možno charakterizovať aj ako permutáciu

$$\pi_s : S_m \to S_m, \quad \pi_s(x) \equiv x^s \pmod m, \tag{5}$$

kde $\mathrm{GCD}(s, \varphi(m)) = 1$ a φ je známa Eulerova funkcia, udávajúca počet čísel neprevyšujúcich m a s ním nesúdeliteľných. Iterovaný útok spočíva v opakovanej aplikácii permutácie π_s:

$$\pi_s^{k+1}(x) = \pi_s(\pi_s(\ldots \pi_s(x))\ldots) = x^{s^{k+1}} = x^s = \pi_s(x), \tag{6}$$

takže $\pi_s^k(x)$ musela byť pôvodná správa. Niekedy sa hovorí aj o k-útoku.

Je prirodzené položiť si nasledujúce otázky:

- Koľko správ sa nezašifruje, t.j. koľko riešení má rovnica $\pi_s(x) \equiv x$?
- Koľko je takých správ, ktoré vieme „prečítať“ k-útokom, t.j. koľko riešení má rovnica (6)?

Odpoveď je možné nájsť v Schwarzovej práci [6], pravda v celkom iných súvislostiach, a najmä bez aplikácie v kryptológii...

Všetko to opäť súvisí s rozkladom pologrupy S_m na jej maximálne podgrupy. Grupa týchto „špeciálnych“ permutácií je izomorfná s maximálnou podgrupou pologrupy $S_{\lambda(pq)}$, $\lambda(pq) = \mathrm{LCM}(p-1, q-1)$[7]).

Inou prirodzenou otázkou je, ako čo najviac „znepríjemniť život“ potenciálnemu oponentovi, t.j. zvoliť p, q tak, aby už spomínané k bolo veľmi veľké pre väčšinu správ $x \in S_m$. Tento výsledok bol publikovaný v [1].

---

[6]) Schwarz bol vášnivým riešiteľom problémov z časopisu The American Mathematical Monthly, kde sa podobné úlohy z času na čas objavovali.

[7]) λ je známa Carmichaelova funkcia.

Záver

V tomto krátkom príspevku sme nespomenuli minimálne ešte jeden výsledok: Jedná sa o tzv. Berlekampovu maticu, ktorá má mimoriadny význam pri realizácii násobenia prvkov konečného poľa na počítači. Pri písaní svojej práce sa von Zur Gathen zaujímal o autorstvo už spomínanej matice, lebo táto sa vyskytuje v Schwarzových prácach skôr než v Berlekampových. Pri tejto príležitosti Schwarz upozornil von Zur Gathena, že túto používal už profesor Petr, ktorého Schwarz považoval za svojho školiteľa. Avšak Petr ani Schwarz neuvažovali o jej praktických aplikáciach. To postrehol až Berlekamp. U samotného Schwarza je to zhodné s jeho prístupom: *Maximálna snaha o aplikačné príklady počas prednášok a takmer nulová pri písaní vedeckých prác. Tam sa aplikácia = aplikácii v matematike samotnej.* Mohli by sme povedať, že bol veľmi „širokospektrálny" pri popularizácii a výuke matematiky, ale veľmi konzervatívny pri písaní vedeckých článkov z matematiky.

Literatúra

[1] Grošek, O.: *Remarks concerning RSA-Cryptosystem exponents.* Math. Slovaca *44,* 2 (1994), 279–285.

[2] Grošek, O.: *On a reconstruction of a Markov Chain.* J. Combin. Inform. System Sci. *20,* 1–4 (1995), 85–93.

[3] Prange, E.: *Cyclic Error-Correcting Codes in Two Symbols.* AFCRC–TN–57–103. Air Force Cambridge Research Center, Cambridge, Mass.

[4] Schwarz, Š.: *Teória pologrúp.* Sborník prác z Prírodovedeckej Fakulty Slovenskej Univerzity v Bratislave, 6 (1943), 64 strán.

[5] Schwarz, Š.: *On the structure of the semigroup of Stochastic Matrices.* Publ. of the Math. Inst. of the Hungarian Academy of Sciences *9,* 3 (1965), 297–311.

[6] Schwarz, Š.: *The role of semigroups in the elementary theory of numbers.* Math. Slovaca *31,* 4 (1981), 309–395.

[7] Thierrin, G.: *Sur les éléments inversifs et les éléments unitaires d'un demi-grupe inversif.* C. R. Acad. Sci. Paris *234* (1952), 177–179.

[8] Vagner, V. V.: *Obobščennyje gruppy.* Dokl. Akad. Nauk SSSR *84* (1952), 1119–1122.