South Bohemia Mathematical Letters
Volume 25, (2017), No. 1, 28-33.

DVA POHLEDY NA JEDNU APLIKACI TEORIE ČÍSEL

JAROSLAV HORA, MARTINA KAŠPAROVÁ, ŠÁRKA PĚCHOUČKOVÁ

ABSTRAKT. Teorie čísel byla kdysi považována za disciplínu zcela neužitečnou, dnes má ale důležité aplikace v šifrování zpráv. Článek obsahuje řadu informací o tomto vývoji, zpracovaných formou užitečnou pro učitele matematiky či zájemce o teorii čísel.

Matematici se na teorii čísel dlouho dívali jako na odvětví své vědy, které nemůže „být k přímému užitku“, jako na neužitečný koníček, který realizujeme po hlavním zaměstnání. Velký anglický matematik G. H. Hardy (1877 – 1947) napsal v roce 1940 v eseji Obrana matematikova: „Je –li matematika královnou věd, pak je teorie čísel, díky své naprosté zbytečnosti, královnou matematiky“.

Jenomže dnes v souvislosti s rozvojem počítačů a s rychle rostoucí potřebou neveřejné komunikace stále širšího okruhu zájemců velice vzrostla potřeba šifrovat zprávy. Teorie čísel v této oblasti našla velice důležité využití. Bylo by možné o tomto relativně novém a nečekaném užití matematiky informovat talentované žáky a na vyšší úrovni i jejich budoucí učitele?

Na FPE ZČU již řadu let probíhá tzv. Dětská univerzita (DU). Jde o soubor kurzů z mnoha různých oborů, které mají zaujmout talentované žáky zhruba ve věku 10 –14 let. Výuka probíhá na podzim v odpoledních hodinách a v kursu O prvočíslech a šifrování se první z autorů tohoto textu věnuje nejprve řešení následující úlohy:

Za první světové války rozbil jednou granát sochu vojáka ze starých dob, držícího v ruce píku. Stalo se to posledního dne v měsíci. Vynásobíme –li postupně čísla
kolikátého dne v měsíci se to stalo,
délku píky ve stopách,
věk kapitána, který tenkrát velel,
polovinu let, po něž socha stála (postavena byla téhož roku, kdy voják na ní znázorněný padl), dostáváme číslo 451 066.
Podivná otázka: Jak starý byl kapitán?

Je vcelku zřejmé, že při řešení této dobře vymyšlené úlohy postačí nalézt faktorizaci čísla 451 066 = 2 . 7 . 11 . 29 . 101. Pak již šikovní frekventanti Dětské univerzity s radostí odpoví, že socha byla rozbita 29. 2. 1916, že délka píky (tj. malého kopí) byla 7 stop, čili asi 2,10 metru, že kapitánu bylo 22 let a socha stála po 202 let.

Při řešení této úlohy vznikl např. problém, zda je číslo 101 prvočíslem. Připomeneme si pojem prvočísla, resp. složeného čísla a přistoupíme k „lovu“ malých prvočísel pomocí Eratosthenova síta. V rozdaných tabulkách obsahujících přirozená čísla od 1 do 150 zapsaná v deseti sloupcích nahlédneme, že si můžeme usnadnit i vyškrtávání např. násobků čísla 2. Ve druhém sloupci bude zřejmě jediné prvočíslo, totiž číslo 2, ve sloupci čtvrtém, šestém, osmém a desátém se prvočísla nenacházejí vůbec, a proto tyto sloupce můžeme vyškrtnout zcela.

Key words and phrases. Eratosthenovo síto, šifrování zpráv, testování prvočíselnosti.
Sieve of Eratosthenes, message encryption, primality testing.

Obdobně v pátém sloupci se nachází, jak se brzy zjistí, jediné prvočíslo 5 a zbytek sloupce lze opět vyškrtnout, tentokrát proto, že obsahuje v dalším již jen násobky pěti. Brzy se stane zřejmým, že „větší množství prvočísel“ se nachází jen v prvním, třetím, sedmém a devátém sloupci.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30

TABULKA 1. Prvních třicet přirozených čísel seřazených po deseti.

Frekventanti DU brzy dokončí svou práci, tj. nalezení všech prvočísel p, kde $1 < p < 150$. Podívejme se však na tuto práci z pohledu vyššího, z pohledu přípravy budoucích učitelů matematiky. Ti dobře vědí, že prvočísel je nekonečně mnoho. Odstraňme nyní horní hranici 150 a zamysleme se nad otázkou, zda by se v množinách přirozených čísel tvaru $10\,n + 1$, $10\,n + 3$, $10\,n + 7$, $10\,n + 9$, $n \geq 0$ nacházelo vždy nekonečně mnoho přirozených čísel. (Obdobně si můžeme představit např. uspořádání do šesti sloupců či obecně do d sloupců, d přirozené číslo). Dostáváme otázku:

Nechť a a d jsou dvě nesoudělná přirozená čísla. Existuje v každé aritmetické posloupnosti tvořené prvky tvaru $a + d\,n$, $n \in \mathrm{N}_0$ nekonečně mnoho prvočísel?

Od „běžného“ Eratosthenova síta jsme se dostali k hlubokému problému z teorie čísel. Kladnou odpověď dal a dokázal až Dirichlet v roce 1837, ale jeho důkaz využívá teorii funkcí komplexní proměnné a je proto považován za neelementární. S elementárním důkazem přišel až A. Sjeberg v r. 1949, to ale neznamená, že jde o důkaz jednoduchý. Vidíme velice názorně, že v teorii čísel se můžeme velice snadno dostat k velice hlubokým problémům.

Žáci navštěvující DU by asi očekávali, že v jejich čtyřech na prvočísla bohatých množinách přirozených čísel tvaru $10\,n + 1$, $10\,n + 3$, $10\,n + 7$, $10\,n + 9$, $n \geq 0$ by se ono nekonečné množství prvočísel mělo rozložit „nějak spravedlivě“, čili v kterékoli z těchto množin by např. nemělo být „mnohem více“ prvočísel než v jiné. Moderní matematika (viz [3], str. 12–13), poskytla zjemnění Dirichletovy věty v tomto smyslu. Označme $\pi(x)$ počet prvočísel nepřevyšujících x a $\pi(x;\ d,\ a)$ počet prvočísel nepřevyšujících x a nacházejících se v aritmetické posloupnosti $\{\ a + n\,d,\ n = 0,\ 1,\ \ldots\}$, kde a, d jsou nesoudělná celá čísla. Pak platí $\lim_{x\to\infty} \frac{\pi(x;\,d,a)}{\pi(x)} = \frac{1}{\varphi(d)}$, kde $\varphi(d)$ značí hodnotu Eulerovy funkce, tj. počet přirozených čísel v intervalu $\langle 1, d\rangle$, nesoudělných s d. (Je hezké vidět, že intuitivní dětská touha po spravedlnosti pro jednou alespoň v jednom oboru lidské činnosti zvítězila).

S žáky v DU realizujeme ještě vyluštění šifry kapitána Kidda. Vše je podrobně popsáno v povídce E. A. Poea The Gold Bug (překládáno jako Zlatý brouk či Zlatý skarabeus). Klíčem k nalezení pokladu je vyluštění následující šifry:

53++!305))6*;4826)4+.)4+);806*;48!8`60))85;;]8*;:+*8!83(88)5*!;
46(;88*96*?;8)*+(;485);5*!2:*+(;4956*2(5*-4)8`8*;4069285);)6
!8)4++;1(+9;48081;8:8+1;48!85;4)485!528806*81(+9;48;(88;4(+?3 4;48)4+;161;:188;+?;

Můžeme předpokládat, že šifra obsahuje sdělení v anglickém jazyce (Kidd byl Angličan) a že každý znak v šifře značí nějaké písmenko anglické abecedy. S mírnou nápovědou se předložená šifra přestane jevit beznadějnou. Nejfrekventovanějším znakem v šifře je 8 a nejfrekventovanějším písmenem v běžném anglickém textu je e. Zdá se proto vhodným

nahradit znak 8 právě písmenem e, což lze provést ve Wordu povelem Nahradit. Dále se v angličtině vyskytuje určitý člen the a v naší šifře je sedm skupin ;48. Lze se domnívat, že středník ; znamená t, 4 znamená h, 8 (jak jsme již vyzkoušeli) znamená e. Po provedení záměn dostaneme

53++!305))6*the26)h+.)h+)te06*the!e`60))e5tt]e*t+*e!e3(ee)5*!t
h6(tee*96*?te)*+(the5)t5*!2:*+(th956*2(5*-h)e`e*th0692e5)t)6
!e)h++t1(+9the0e1te:e+1the!e5th)he5!52ee06*e1(+9**thet(eeth**(+?3 hthe)h+t161t:1eet+?t

Poté se již objevuje skupina the t(ee th.. a v ní zřejmě bude slovo tree, tj. (asi značí r a šifra se postupně začne vyjasňovat. Vše je ostatně popsáno ve výše zmíněné povídce, kterou lze najít i na internetu. Definitivní anglický text po oddělení jednotlivých slov zní:

A good glass in the bishop's hostel in the devil's seat twenty-one degrees and thirteen minutes northeast and by north main branch seventh limb east side shoot from the left eye of the death's-head a bee-line from the tree through the shot fifty feet out.

Hrdina povídky si ještě domyslí, že zprávu je třeba rozdělit pomlčkami v určitých místech, kde se pisatel šifry naopak naivně snažil text zhustit, a dostane výsledný text, který uvádíme v českém překladu:

Dobré sklo v biskupově hospodě na ďáblově stolici – jednadvacet stupňů a třináct minut – severoseverovýchodně – hlavní větev sedmá větev východní strana – vystřel z levého oka umrlčí hlavy – přímo od stromu z místa dopadu na padesát stop.

Tím je přilákána pozornost žáků z Dětské univerzity k šifrování. Ukázalo se, že tzv. substituční šifra není neprolomitelná. Skončíme konstatováním, že dnes již nepotřebují šifrovat jen vojáci a diplomaté, ale skoro každý, protože bychom nebyli rádi, kdyby se někdo cizí mohl dostat k třeba našim bankovním údajům či daňovým přiznáním. Dnes se o bezpečnost takovýchto zpráv stará matematika a využívá se velkých prvočísel. Je snadné rozložit např. číslo 35 = 5.7 na součin dvou prvočísel, ale kdybychom vzali dvě opravdu veliká prvočísla p, q a na počítači spočítali jejich součin, pak by pro nepřítele bylo velice těžké objevit původní prvočísla. Zde je pochopitelně potřeba skončit s tím, že více se o těchto záležitostech dozvíme později, na střední či spíše vysoké škole.

Budoucí učitelé však mají z kursu elementární algebry připraveno vše podstatné k pochopení tzv. RSA šifrovací metody (autory jsou Rivest, Shamir a Adlemann). Jak tato metoda funguje? Nejprve je zapotřebí převést zprávu z běžného jazyka do posloupnosti čísel, což lze snadno učinit. Obdržíme jakési číslo x. Nyní je třeba vzít dvě „veliká“ navzájem různá prvočísla p, q. Jejich součin $p.q$ je pochopitelně rozumné spočítat na počítači. Tento součin nebude nijak utajován, lze jej kupř. zveřejnit v novinách.

Ten, kdo zná obě prvočísla p a q, může velice snadno spočítat hodnotu Eulerovy funkce $\varphi(p.q) = (p-1)\,(q-1)$. Nyní zvolí nějaké číslo e nesoudělné s $\varphi(p.q)$, nikoli však $e = 1$ nebo $e = (p-1)\,(q-1) - 1$. Toto číslo (šifrovací exponent) se též zveřejní. Každý, kdo zná čísla $p.q$ a e, může své sdělení zašifrovat (proto se mluví o metodě veřejného klíče). Provede to tak, že vypočte (ovšemže opět s pomocí počítače) číslo y, pro něž platí $y \equiv x^e \pmod{p.q}$. Autor kódu si musí vypočítat ještě jedno číslo (dekódovací exponent f, „tajný“ klíč). Nalezne jej jako řešení kongruence $e.f \equiv 1 \pmod{\varphi(p.q)}$.

To není obtížný úkol, neboť čísla e, $\varphi(p.q)$ jsou, jak řečeno, nesoudělná, $D(e, \varphi(p.q)) = 1$. Hledání čísla f se opírá o tzv. rozšířený Euklidův algoritmus, tj. o to, že existují celá čísla f, h taková, že $e.f + \varphi(p.q).h = 1$. Je pak $e.f = 1 - \varphi(p.q).\,h$, čili $e.f - 1$ je dělitelné $\varphi(p.q)$ a $e.f \equiv 1 \pmod{\varphi(p.q)}$.

Nyní již můžeme dešifrovat. Předpokládejme, že pro původní číslo x platí, že $x < p.q$ (kdyby to nebylo splněno, bylo by možné původní zprávu rozdělit na více částí) a že ani p, ani q nedělí x (prakticky vzato, tento příklad pro „veliká“ prvočísla p, q nastane „málokdy“ a problém lze vždy obejít malou úpravou x, která nemění smysl zprávy).

Jak víme, platí $e.f = 1 - \varphi(p.q).\ h$, nebo, pokud označíme $k = -h$, $e.f = 1 + \varphi(p.q).\ k$. Víme dále, že čísla x a $p.q$ jsou nesoudělná, takže podle Eulerovy věty

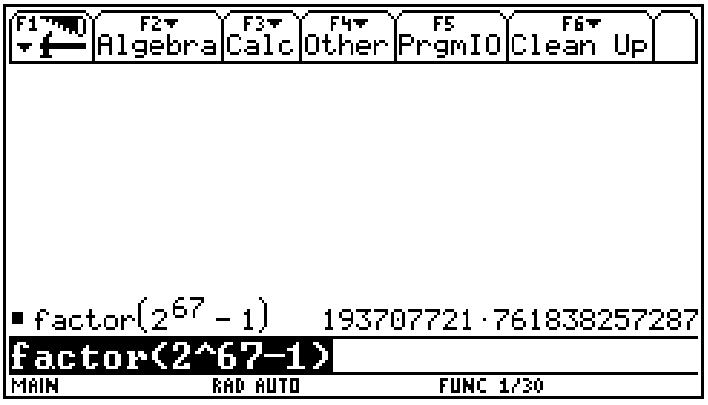
$$x^{\varphi(p.q)} \equiv 1 \pmod{p.q}$$

a tedy též $$x^{k.\varphi(p.q)} = \left(x^{\varphi(p\cdot q)}\right)^k \equiv 1 \pmod{p.q}$$

a nakonec $y^f = x^{e.f} = x.\ x^{k.\varphi(p.q)} \equiv x \pmod{p.q}$.

Poslední vztah popisuje, jak zakódované slovo y dešifrovat – postačí vypočítat nejmenší nezáporný zbytek při dělení mocniny y^f modulem $p.q$. To je, jak víme, efektivně řešitelná úloha.

Možnosti výpočetní techniky a objev RSA šifrovací metody samozřejmě způsobily výrazný pokrok v metodách užívaných v teorii čísel. Následující příklad je ilustrativní. Americký matematik F. N. Cole (1861 – 1926), profesor na Columbia University a sekretář Americké matematické společnosti, se dne 31. 10. 1903 proslavil faktorizací Mersennova čísla $2^{67} - 1 = 147573952589676412927 = 761838257287 \times 193707721$. Výpočty provedl beze slov křídou na velké tabuli a byl kolegy odměněn potleskem vestoje. Později přiznal, že mu nalezení této faktorizace zabralo „tři roky nedělí“. Dnes jsou k dispozici lepší faktorizační algoritmy a výpočetní technika, takže např. kalkulátor TI-92 Plus nalezne tento rozklad do dvou minut (viz obr. 1). Velmi zajímavou stránku nabízející faktorizaci s využitím metody eliptických křivek nalezne čtenář na https://www.alpertron.com.ar/ECM.HTM.



OBRÁZEK 2. Výpočet na kalkulátoru TI-92

Starší generace dnešních učitelů matematiky bývala za svých studií krátce seznamována jen se školní metodou opakovaného dělení. Ta je zároveň faktorizační metodou a zároveň prvočíselným testem. Je – li totiž zadáno přirozené číslo n, můžeme testovat jeho dělitelnost (prvo)čísly 2, 3 … atd. do největšího přirozeného čísla k, pro které ještě platí $k \leq \sqrt{n}$. Najdeme-li při tomto testování dělitel čísla n, jde o číslo složené a získali jsme rovněž dělitel čísla n; jinak je číslo n prvočíslem. Je potřeba si uvědomit, že dnes existuje řada faktorizačních metod a poněkud se snižuje jejich výpočetní složitost, ale stále jde o „těžkou“ úlohu a právě na tomto faktu je založena RSA šifrovací metoda. Testování prvočíselnosti je samostatným problémem a jeho výpočetní složitost je nižší.

Podle malé Fermatovy věty platí pro každé prvočíslo p a každé celé číslo a konguence

$$a^p \equiv a \pmod{p}. \qquad (1)$$

Pokud je a nesoudělné s p, lze v předchozí kongruenci krátit a platí

$$a^{p-1} \equiv 1 \pmod{p}. \qquad (2)$$

Volbou $a = 2$ dostáváme tvrzení, že pokud p je prvočíslo, pak p dělí $2^{p-1} - 1$. Neplatí zde dokonce ekvivalence? Jak se uvádí v [5], věřil v platnost této hypotézy i G. W. Leibniz. (Tyto informace jsou však dnes i zpochybňovány; viz [4]). Ať tak či onak, je zajímavé to otestovat pro čísla větší nebo rovná třem. Vskutku, platí ekvivalence

3 je prvočíslo $\Leftrightarrow$ 3 dělí $2^2 - 1$;
4 není prvočíslo $\Leftrightarrow$ 4 nedělí $2^3 - 1$;
5 je prvočíslo $\Leftrightarrow$ 5 dělí $2^4 - 1$;
6 není prvočíslo $\Leftrightarrow$ 6 nedělí $2^5 - 1$;
7 je prvočíslo $\Leftrightarrow$ 7 dělí $2^6 - 1$;
8 není prvočíslo $\Leftrightarrow$ 8 nedělí $2^7 - 1$;
9 není prvočíslo $\Leftrightarrow$ 9 nedělí $2^8 - 1$;
10 není prvočíslo $\Leftrightarrow$ 10 nedělí $2^9 - 1$;
11 je prvočíslo $\Leftrightarrow$ 11 dělí $2^{10} - 1$ atd.

Snad bychom byli i my ochotni uvěřit... . Ani velký počet úspěšných testů není důkazem obecného matematického tvrzení! Platnost hypotézy se skutečně naruší, nastane to však až pro $n = 341$, kdy jde o číslo složené ($341 = 11.31$), ale 341 dělí $2^{340} - 1$. Tak byla objevena složená čísla, která procházejí tzv. 2 – prvočíselným testem (tzv. pseudoprvočísla o základu 2). Je jich jen 7 menších než 2 000, konkrétně 341, 561, 645, 1 105, 1 387, 1 729, 1 905.

Zkusme změnit základ a testovat např. v programu Mathematica platnost malé Fermatovy věty pro $a = 3$. Vidíme, že problém nastane tentokrát brzy.

```
For[n = 2,n < 2000, n=n+1,
 If[Xor[PrimeQ[n], IntegerQ[(3^n-3)/n]], Print[n]]]
6
66
91
121
286
561
671
703
726
949
1105
1541
1729
1891
```

Nyní zjistíme snadno i zpaměti, že složené číslo 6 splňuje vztah (1), tj. platí kongruence $3^6 \equiv 3 \pmod 6$. Z malé Fermatovy věty jsme věděli, že $3^p \equiv 3 \pmod p$ platí pro všechna prvočísla p, ale nyní jsme nahlédli, že kongruence (1) platí i pro složené číslo 6. Malá Fermatova věta tedy neposkytne prvočíselný test ani pro základ $a = 3$.

Řekneme, že složené číslo n je (Fermatovým) pseudoprvočíslem o základu a, pokud platí $a^n \equiv a \pmod n$.

Mnohem horší je, že nacházíme složená čísla, která se vyskytují jako pseudoprvočísla v obou našich seznamech. Mohli bychom ovšem přejít k dalšímu základu a a nechat počítač zpracovat další seznam. Ani to nepomůže. Existují naneštěstí i složená přirozená čísla n, pro která platí kongruence $a^n \equiv a \pmod n$ pro každé celé číslo a. Tato čísla se nazývají Carmichaelova čísla po matematikovi, který objevil první z nich v roce 1910. Pozoruhodné je, že prvních sedm Carmichaelových čísel (561, 1 105, 1 729, 2 465, 2 821, 6 601, 8 911) nalezl již český matematik V. Šimerka v roce 1885, ale jeho česky psaná práce [6] zůstala zřejmě nepovšimnuta. Teprve v roce 1994 bylo v práci [2] dokázáno, že je těchto čísel nekonečně mnoho. Bylo vypracováno mnoho dalších prvočíselných testů (nemusíme totiž využívat jen

malou Fermatovu větu), ale v jejich popisu nebudeme pokračovat (viz např. [3]). V roce 2002 zveřejnila trojice mladých indických matematiků článek [1], ve kterém je popsán nový deterministický test prvočíselnosti, pracující s polynomy nad konečnými tělesy. Tento test je velice významný z teoretického hlediska, neboť jde o první algoritmus určující v polynomiálním čase, zda je dané číslo prvočíslem nebo složeným číslem. Za tuto práci získali autoři v r. 2006 hned dvě ceny, a to Gödelovu a Fulkersonovu cenu.

Zmiňme se na závěr o postupu, kterým lze vygenerovat prvočíslo mající předem daný počet cifer. Lze využít Pocklingtonovo kritérium:

Nechť p je liché prvočíslo a k je přirozené číslo, které není dělitelné p a platí $1 \le k \le 2(p + 1)$. Nechť $N = 2kp + 1$. Pak jsou následující tvrzení ekvivalentní:

1) N je prvočíslo
2) Existuje přirozené číslo a, $1 \le a < N$ takové, že $a^{kp} \equiv -1 \pmod{N}$ a $D(a^{k+1}, N) = 1$.

Důkaz tohoto tvrzení a množství dalších informací nalezne čtenář ve vtipně psaném článku [5]. Poznamenejme, že pokud volíme např. $p = 5$ (jednociferné prvočíslo), pak pro $k = 6$ máme $N = 61$ (dvojciferné prvočíslo) a uspějeme hned s volbou $a = 2$: ve shodě s bodem 2) Pocklingtonova kritéria je $2^{30} \equiv -1 \pmod{61}$ a $D(2^7, 61) = 1$. Vtip je ale v tom, že kdyby nám počítač pomohl s nalézáním vhodných čísel k, a, (to naštěstí dobře funguje), mohli bychom zhruba zdvojnásobovat velikost prvočísel a generovat si velká prvočísla „na míru“, což je jistě příhodné pro realizaci RSA šifrování.

ZÁVĚR

I teorie čísel dnes nalezla významné praktické užití a je v ní řada podnětů zajímavých pro studenty se zájmem o matematiku.

LITERATURA

[1] Agrawal, M., Kayal, N., Saxena, N.: *PRIMES is in P*, Annals of Mathematics, 160 (2), (2004), 781–793.

[2] Alford, W. R., Granville, A., Pomerance, C.: *There are Infinitely Many Carmichael Numbers*. Annals of Mathematics, vol. 139 (1994), No. 3, pp. 703-722.

[3] Crandall, R., Pomerance, C.: *Prime Numbers. A Computational Perspective*. Second Edition, Springer, 2005.

[4] Křížek, M., Somer, L.: *Pseudoprvočísla*. Pokroky matematiky, fyziky a astronomie, vol. 48 (2003), issue 2, pp. 143-151.

[5] Ribenboim, P.: *Selling Primes*, Mathematics Magazine, Vol. 68, No. 3 (Jun., 1995), pp. 175-182.

[6] Šimerka, V.: *Zbytky z aritmetické posloupnosti*. Časopis pro pěstování matematiky a fysiky, r. 1885, 14 (5): 221–225.

[7] Veselý, F.: *O dělitelnosti čísel celých*. Škola mladých matematiků, No 14, Mladá fronta, Praha, 1966.

KATEDRA MATEMATIKY, FYZIKY A TECHNICKÉ VÝCHOVY FPE ZČU PLZEŇ, ČESKÁ REPUBLIKA

E-mail address: horajar@kmt.zcu.cz, mernesto@kmt.zcu.cz, pechouck@kmt.zcu.cz