MUNDUS SYMBOLICUS 19 (2011)

Jeskyně Třináctka

Jiří Nečas

Abstract. ***The grotto Thirteen.*** This article uses the form of a fairy tale; it introduces the basic topics and operations in a finite field, especially in the field of residual classes of module 13 with emphasis on the fact, that this field is unordered. Besides main field operations the tale deals with exponentiation and discrete logarithm, too.

Pohádka, která seznamuje s počítáním v tělese zbytkových tříd podle modulu 13.

Vítám vás, milí čtenáři, opět v pohádkovém lese [1], [2]. Setkáme se zase s krásnou a sympatickou princeznou Alguelitou[1] i s vílami a kovílasy[2]. Ke správnému pohádkovému lesu patří jeskyně. Nechybí ani u nás. Spolu se skupinou dětí řešících pytagoriádu jeskyni Třináctku navštívíme.

A jako já coby autor vítám čtenáře, tak princezna Alguelita uvítala skupinu matematikychtivých dětí[3] u vchodu do Třináctky. Čtenář, který není v našem pohádkovém lese ponejprv, už ví, že krásná a vzdělaná princezna Alguelita, matematicky vzdělaná zooložka a ekoložka, se svými krásnými dlouhými kaštanovými vlasy, velkýma dobro vyzařujícíma očima, milým úsměvem, cudností a skromností se svým tradičním pohádkovým kolegyním - princeznám podobá, avšak místo nepraktických princeznovských šatů nosívá kalhoty a tričko, a je to taková inteligentní a laskavá intelektuálka. Tentokrát měla na sobě kalhoty béžové a modré tričko, na němž byly vpředu zobrazeny dvě velké soustředné kružnice. Dětem to trochu připomínalo orloj, nicméně princezna byla tak milá a tak krásně a zajímavě povídala, že jim z jeskyně myšlenky na pražské Staroměstské ani na olomoucké Horní náměstí neutíkaly. Vnitřní kružnice byla žlutá a připomínala ciferník hodin; měla po obvodě vyznačených dvanáct bodů, označených obdobně jako celé hodiny na hodinách, avšak dva rozdíly byly nápadné. Onen horní bod měl označení dvě – nulu a dvanáctku, kterou vyjadřovalo písmeno C. Princezna si totiž uvědomila, že by bylo docela nerozumné, když pracujeme s čísly do dvanácti, používat dvojciferná čísla, a tak shodně s konvencí programátorů z reálného světa používala pro desítku písmeno A, pro jedenáctku B

[1] Princezna je představena v [2], v [1] vystupuje princezna bez jména. Princeznino jméno, inspirované jménem autorky knihy [4], poukazující na možnosti pohádky pro sdělování, vyjadřuje důležitost řas pro globální ekosystém; alga je latinsky a španělsky řasa; španělsky tvořená dvojnásobná zdrobnělina příponou *-uelita* je Algüelita, do češtiny přepisujeme Alguelita.

[2] Mužská obdoba víly. Český slovní základ *víl* je doplněn předponou *ko-* s obdobným významem jako u goniometrických funkcí a příponou *-a*s, která je převzata z litevštiny jako základní příznak maskulina (tam jde o nominativní pádovou koncovku).

[3] Dětem jsou zde přisuzovány znalosti, které se očekávají až od středoškoláků. Autor se za to omlouvá, avšak do pohádky se lépe hodí děti než mládež

a pro dvanáctku C. Vnější, červená kružnice měla po obvodě vyznačeno třináct rovnoměrně od sebe vzdálených bodů. Horní bod byl označen 0, a pak, proti směru hodinových ručiček, byly body 1, 2,..., B, C.

A jak princezna děti přivítala? Pověděla jim, že si váží toho, jak zvládly počítání s čísly[4]. Říše čísel je krásná, bohatá, dokonce bohatší než všechno lidské poznání světa. Při tom jim slíbila, že v jeskyni najdou jiný svět. Bude se v něm počítat obdobně jako se v lidském světě počítá s reálnými čísly, avšak v jeskynním světě bude čísel konečně mnoho, jak už napovídá název jeskyně – Třináctka. Ano, hlavní větev matematiky v Třináctce vystačí s třinácti čísly, kterým se říká ***trettočísla***[5]. A jedno z nich − nula − je docela nezajímavé. A tak je v Třináctce dvanáct zajímavých čísel.

Alguelita vyjádřila naději, že chytré děti nejsou pověrčivé. A kdyby snad některé přece jen pověrčivé bylo a před třináctkou mělo takový mrazivý respekt, ať raději myslí na těch dvanáct zajímavých trettočísel.

U vstupu do jeskyně Třináctky Alguelita představila dětem jejich průvodce světem trettočísel: víly Algebru a Exponenciálu a kovílasy Modula a Logaritma. Pak děti doprovodila do úžasné podzemní síně a tam předala slovo víle Algebře.

Algebra dětem zopakovala ve velkolepé jeskyni pohádkového světa pravidla, která splňuje počítání s čísly v lidském světě. Připomeňme si je spolu s nimi.

Pro sčítání platí:

sk) Pro libovovolná dvě čísla a, b je $a + b = b + a$.

sa) Pro libovolná tři čísla a, b, c je $(a + b) + c = a + (b + c)$.

sn) Existuje právě jedno číslo 0, pro něž pro libovolné číslo a platí $0 + a = a$.

si) Ke každému číslu a existuje právě jedno takové číslo $-a$, že platí $a + -a = 0$.

Číslo 0 nazýváme nula, číslo $-a$ je opačné číslo k číslu a.

Poslední pravidlo (si) nám umožňuje definovat odčítání: Pro libovolná dvě čísla a,b definujeme jejich rozdíl $a - b = a + -b$.

Podobná pravidla platí pro násobení:

mk) Pro libovolná dvě čísla a, b je $a \,.\, b = b \,.\, a$.

ma) Pro libovolná tři čísla a, b, c je $(a.b).c = a.(b.c)$.

mn) Existuje právě jedno číslo 1, pro něž pro libovolné číslo a platí $1 \,.\, a = a$.

mi) Ke každému číslu a , různému od nuly existuje právě jedno takové číslo a^{-1}, že platí $a.a^{-1} = 1$.

Číslo 1 nazýváme jednotka, číslo a^{-1} je převrácené čili inverzní číslo k číslu a.

Poslední pravidlo (mi) nám umožňuje definovat dělení nenulovým číslem: Pro libovolné číslo a a libovolné nenulové číslo b definujeme jejich podíl $a / b = a \,.\, b^{-1}$.

A samozřejmě, že víla Algebra připomněla i distributivní zákon a jednu důležitou vlastnost nuly:

d) Pro libovolná tři čísla a, b, c je $(a + b).c = a.c + b.c$.

z) Pro každé číslo a platí $0.a = 0$.

---

[4] Číslem rozumíme reálné číslo (případně racionální číslo).

[5] Tretton je švédsky třináct.

I když takovouto teorii ani děti milující matematiku ve škole nemají v žádné zvláštní oblibě, v podání víly Algebry vše poslouchaly úplně se zatajeným dechem. A jejich poznáníchtivost ještě vzrostla, když se Algebra zmínila, že pro platnost těchto pravidel pro počítání není podstatné, že (lidských) čísel je nekonečně mnoho. Ale to už předala slovo kovílasovi Modulovi. Jeho plné jméno je *Modul Třináct*, ale on je zvyklý na to, že se mu říká krátce Modul. A tak i zde o něm jako o Modulovi budeme mluvit.

Modul přišel s tím, že v Jeskyni Třináctce počítají s *trettočísly*, sčítají je a násobí, a také odčítají a dělí (nulou ovšem nikoli). Je jich třináct, od nuly do dvanáctky (ale také bychom mohli říci třeba od pětky do čtyřky, přičemž po dvanáctce následuje nula). A jak už víme z Alguelitina trička, desítka, jedenáctka a dvanáctka se označují jednociferně A, B, a C. A protože trettočísel je konečně mnoho, mohou se operace mezi nimi definovat tabulkami. Rychle na plátno v čele jeskyně promítl tabulky sčítání a násobení a vyzval děti, aby si je dobře prohlédly:

SČÍTÁNÍ TRETTOČÍSEL

+	0	1	2	3	4	5	6	7	8	9	A	B	C
0	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**
1	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**0**
2	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**0**	**1**
3	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**0**	**1**	**2**
4	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**0**	**1**	**2**	**3**
5	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**0**	**1**	**2**	**3**	**4**
6	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**0**	**1**	**2**	**3**	**4**	**5**
7	**7**	**8**	**9**	**A**	**B**	**C**	**0**	**1**	**2**	**3**	**4**	**5**	**6**
8	**8**	**9**	**A**	**B**	**C**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
9	**9**	**A**	**B**	**C**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
A	**A**	**B**	**C**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
B	**B**	**C**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**
C	**C**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**

NÁSOBENÍ TRETTOČÍSEL

.	0	1	2	3	4	5	6	7	8	9	A	B	C
0	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
1	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**
2	**0**	**2**	**4**	**6**	**8**	**A**	**C**	**1**	**3**	**5**	**7**	**9**	**B**
3	**0**	**3**	**6**	**9**	**C**	**2**	**5**	**8**	**B**	**1**	**4**	**7**	**A**
4	**0**	**4**	**8**	**C**	**3**	**7**	**B**	**2**	**6**	**A**	**1**	**5**	**9**
5	**0**	**5**	**A**	**2**	**7**	**C**	**4**	**9**	**1**	**6**	**B**	**3**	**8**
6	**0**	**6**	**C**	**5**	**B**	**4**	**A**	**3**	**9**	**2**	**8**	**1**	**7**
7	**0**	**7**	**1**	**8**	**2**	**9**	**3**	**A**	**4**	**B**	**5**	**C**	**6**
8	**0**	**8**	**3**	**B**	**6**	**1**	**9**	**4**	**C**	**7**	**2**	**A**	**5**
9	**0**	**9**	**5**	**1**	**A**	**6**	**2**	**B**	**7**	**3**	**C**	**8**	**4**
A	**0**	**A**	**7**	**4**	**1**	**B**	**8**	**5**	**2**	**C**	**9**	**6**	**3**
B	**0**	**B**	**9**	**7**	**5**	**3**	**1**	**C**	**A**	**8**	**6**	**4**	**2**

C	**0**	**C**	**B**	**A**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**

Obě tabulky jsou symetrické[6] – mezi trettočísly tak platí pro sčítání i pro násobení komutativní zákony sk, mk. Proto je také lhostejno, zda první operand hledáme v levém sloupci a druhý v horním řádku či naopak. Z toho, jak vypadá řádek náležející nule u sčítání a jedničce u násobení, je vidět, že zde platí i zákony sn a mn. V tabulce sčítání je v každém řádku právě jednou nula – ta je právě ve sloupci, v jehož záhlaví je trettočíslo opačné k číslu v záhlaví příslušného řádku. Můžeme si tak vytvořit tabulku opačných čísel:

a	0	1	2	3	4	5	6	7	8	9	A	B	C
-a	0	C	B	A	9	8	7	6	5	4	3	2	1

Z řádku či ze sloupce odpovídajícího nule vidíme, že zde platí zákon z, a tedy k nule neexistuje inverzní trettočíslo. K nenulovým trettočíslům však inverzní trettočísla v tabulce snadno vyhledáme tak, že pro vybrané trettočíslo najdeme příslušný řádek, v něm najdeme jedničku, a ta je ve sloupci, v jehož záhlaví je hledané inverzní trettočíslo. Zde je tabulka inverzních trettočísel:

a	1	2	3	4	5	6	7	8	9	A	B	C
a^{-1}	1	7	9	A	8	B	2	5	3	4	6	C

Při vyjadřování opačných čísel se obejdeme bez znaménka "minus", při vyjadřování převrácených čísel bez zlomků. K násobení a k převráceným trettočíslům obrátíme svou pozornost za chvíli; teď se zamysleme nad tím, zda bychom přece jen nemohli některá trettočísla prohlásit za záporná. Jistě, mohli; jde o to, zda by to bylo rozumné, a jaký přístup by byl nejrozumnější. Jedna možnost by bylo prohlásit za záporná ta čísla, od nichž je (názorně) blíže k nule pomocí přičtení než pomocí odečtení, tedy 7 až C. Modul poznamenal, že podobně to dělají na zemi programátoři, když řeší ukládání celých čísel v počítači, ale když už on by byl těmi zápornost uctívajícími lidmi nucen některá trettočísla prohlásit za záporná, byla by to trettočísla 2, 5, 6, 7, 8 a 11. Proč zrovna takto, vysvětlí pozdější víla Exponenciála. Že by se podobný přístup ve struktuře, již používají programátoři, použít nedal, a i kdyby dal, nebylo by to pro práci počítače vhodné, o tom se Modul už nezmínil.

Měl Modul platnost zbývajících pravidel dětem prostě jen předložit k věření? On jim to dal jako podnět k přemýšlení, přičemž jim prozradil, že součet a součin trettočísel se dá vypočítat tak, že se spočítá jejich součet a součin jako obyčejných lidských čísel, získaný výsledek se vydělí (se zbytkem) třinácti; zbytek při tomto dělení je výsledkem operace mezi trettočísly. Lidé těmto operacím říkají sčítání, resp. násobení podle modulu 13. Díky této souvislosti s počítáním s lidskými čísly se na základě asociativity a distributivity jejich sčítání a násobení dá poměrně snadno dokázat, že tyto vlastnosti mají i operace s trettočísly.

A když můžeme s trettočísly počítat, můžeme v jejich oboru řešit i rovnice. Lineární jsou podle Modula docela nezajímavé, ukázal to na příkladu

$5x = \mathrm{B}$;

[6] Nezmění se, zaměníme-li řádky a sloupce, pokud jejich pořadí zůstane zachováno.

obě strany rovnice vynásobil trettočíslem inverzním k 5, tedy 8:

$8.5x = 8.\mathrm{B},$

tedy

$x = \mathrm{A}.$

Protože se však pohybujeme v konečné, nepříliš početné množině, můžeme k řešení rovnice použít přímo tabulku násobení; v řádku příslušejícím trettočíslu 5 najdeme výsledek B; nachází se ve sloupci trettočísla A.

Poslouchající děti ani neregistrovaly ubíhající čas, přesto však Modulova informace, že teď přijdou ještě zajímavější věci, je potěšila. Než před děti předstoupila usměvavá víla Exponenciála, laskavá Algebra jim připomněla, jak se zavádí nezáporná celočíselná mocnina mezi čísly. Udělala to poctivě, indukcí:

Pro každé číslo a je $a^0 = 1$. Dále definujeme $a^{n+1} = a.a^n$

Exponenciála své pozorné posluchače upozornila, že definice indukcí uvažuje mocnitel jako libovolné přirozené číslo[7]. Mocniny nuly jsou nezajímavé, mocniny nenulových trettočísel jsou zas nenulová trettočísla, a těch je dvanáct; jejich hodnoty se periodicky opakují. Protože nejdelší perioda tohoto opakování je dvanáct, mocnitel budeme vyjadřovat pomocí tolvočísel[8], jichž, na rozdíl od trettoočísel není třináct, nýbrž dvanáct. Tolvočísla nebudeme násobit, budeme je jen sčítat. Jejich sčítání vyjadřuje tato tabulka:

SČÍTÁNÍ TOLVOČÍSEL

+	0	1	2	3	4	5	6	7	8	9	A	B
0	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**
1	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**0**
2	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**0**	**1**
3	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**0**	**1**	**2**
4	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**0**	**1**	**2**	**3**
5	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**0**	**1**	**2**	**3**	**4**
6	**6**	**7**	**8**	**9**	**A**	**B**	**0**	**1**	**2**	**3**	**4**	**5**
7	**7**	**8**	**9**	**A**	**B**	**0**	**1**	**2**	**3**	**4**	**5**	**6**
8	**8**	**9**	**A**	**B**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
9	**9**	**A**	**B**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
A	**A**	**B**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
B	**B**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**

Dvanáctá mocnina je v našem světě trettočísel vždy stejná jako nultá. Protože by někdy vypadalo dost násilně dvanáctku nahrazovat nulou, při počítání s tolvočísly považujeme 0 a C (= 12) za vyjádření téhož čísla.

Vtom se tam ukázala princezna Alguelita a ukázala žlutou kružnici na svém tričku, kde horní bod měl dvě označení, 0 a C. Připomněla, že je to podobné, jako když půlnoc někdy

[7] Tedy nezáporné celé číslo; nulu považujeme tedy za přirozené číslo.
[8] Tolv je švédsky dvanáct.

označujeme jako 0 hodin, někdy jako 24 hodin. Lpět na jednom označení nemusí být vždy nejšikovnější.

Vzápětí však Alguelita zas udělala prostor víle Exponenciále, a ta ukázala tabulku mocnin; v levém záhlaví jednotlivých řádků jsou nenulová trettočísla, sloupce jsou nadepsány tolvočísly; sloupce nadepsané 0 a C jsou (až na grafickou úpravu) stejné. Nultá mocnina i dvanáctá mocnina jsou vždy rovny 1, nula a dvanáctka představují stejné tolvočíslo.

V řádcích odpovídajících trettočíslům 2, 6, 7 a 11 jsou obsažena všechna nenulová trettočísla. Tato trettočísla – tzv. ***primitivní kořeny*** – mohou sloužit jako základ jakéhosi speciálního trettočíslového logaritmu. O tom však bude povídat kovílas Logaritmus.

Exponenciála dále zmínila, že mezi mocninami ostatních trettočísel se vyskytují jen některá trettočísla. Hodnoty mocnin se periodicky opakují, délka periody (říká se též délka cyklu) je vždy dělitelem čísla 12.

MOCNINY TRETTOČÍSEL														
exponent *n*	0	1	2	3	4	5	6	7	8	9	A	B	C	Délka
základ *x*														cyklu
1	**1**	**1**	1	1	1	1	1	1	1	1	1	1	**1**	1
2	**1**	**2**	**4**	**8**	**3**	**6**	**C**	**B**	**9**	**5**	**A**	**7**	**1**	**C**
3	**1**	**3**	**9**	**1**	3	9	**1**	3	9	**1**	3	9	**1**	3
4	**1**	**4**	**3**	**C**	**9**	**A**	**1**	4	3	C	9	A	**1**	6
5	**1**	**5**	**C**	**8**	**1**	5	C	8	**1**	5	C	8	**1**	4
6	**1**	**6**	**A**	**8**	**9**	**2**	**C**	**7**	**3**	**5**	**4**	**B**	**1**	**C**
7	**1**	**7**	**A**	**5**	**9**	**B**	**C**	**6**	**3**	**8**	**4**	**2**	**1**	**C**
8	**1**	**8**	**C**	**5**	**1**	8	C	5	**1**	8	C	5	**1**	4
9	**1**	**9**	**3**	**1**	9	3	**1**	9	3	**1**	9	3	**1**	3
10	**1**	**A**	**9**	**C**	**3**	**4**	**1**	A	9	C	3	4	**1**	6
11	**1**	**B**	**4**	**5**	**3**	**7**	**C**	**2**	**9**	**8**	**A**	**6**	**1**	**C**
12	**1**	**C**	**1**	C	**1**	C	**1**	C	**1**	C	**1**	C	**1**	2

V tabulce mocnin trettočísel ve sloupci exponentu 2 dvakrát vystupují trettočísla 1, 3, 4, 9, A a C jsou to tzv. ***kvadratické zbytky***. Dále víme, že nula je druhou mocninou nuly. Trettočísla 2, 5, 6, 7, 8 a B , která nejsou druhou mocninou žádného trettočísla, nazýváme ***kvadratickými nezbytky***. Vzdáleně to připomíná dělení lidských čísel na kladná a záporná - záporná čísla nejsou druhou mocninou žádného čísla, kladná pak dvou čísel lišících se znaménkem. A i v lidské aritmetice je nula druhou mocninou nuly a žádného jiného čísla.

Teď Exponenciála předala slovo Algebře, aby popovídala o kvadratických rovnicích v oboru trettočísel.

Kvadratická rovnice má, podobně jako mezi obyčejnými čísly, tvar

$a.x^2 + b.x + c = 0,$

kde $a \neq 0$. Protože a je nenulové, můžeme rovnici vynásobit trettočíslem a^{-1} a uvést ji do *normovaného* tvaru

$$x^2 + p.x + q = 0,$$

kterou můžeme převést na tvar

$$(x + 7p)^2 = (7p)^2 - q.$$

Teď se na chvíli víla Algebra odmlčela a čekala, jak se pozorně poslouchající děti budou tvářit na sedmičku. Ale opravdu jen na chviličku, v pohádkovém světě byly všechny poslouchající děti ještě bystřejší než jako řešitelé Pytagoriády, a tak si uvědomily, že násobit 7 je vlastně totéž jako dělit 2; 2 a 7 jsou navzájem inverzní trettočísla

Konstatování, že počet řešení kvadratické rovnice závisí na tom, zda trettočíslo $(7p)^2 - q$ je kvadratický zbytek, nula či kvadratický nezbytek, už nikoho nepřekvapil. V prvním případě má rovnice dvě řešení, v druhém jedno a v posledním žádné.

V normované kvadratické rovnici může každý z koeficientů p, q nabývat třinácti různých hodnot. Řešení pro všech 169 různých rovnic (v závislost na p a q) uvádí tabulka. Aby do ní bylo možno zapsat dva kořeny, každému q odpovídají dva sloupce; při dvou kořenech jsou oba využity, při jednom (dvojnásobném) je v pravém symbol −, pokud řešení neexistuje, je v obou sloupcích #.

Pokud máme kvadratickou rovnici v oboru reálných čísel, na jejíž kořeny i koeficienty se můžeme dívat jako na trettočísla, pak v oboru trettočísel má tytéž kořeny.

Řešení kvadratické rovnice $x^2 + px + q = 0$

p \ q	0		1		2		3		4		5		6		7		8		9		A		B		C	
0	0	−	8	5	#	#	7	6	3	A	#	#	#	#	#	#	#	#	B	2	4	9	#	#	1	C
1	C	0	3	9	#	#	#	#	#	#	#	#	8	4	2	A	#	#	5	7	6	−	1	B	#	#
2	0	B	−	C	4	7	#	#	5	6	9	2	#	#	#	#	#	#	#	#	1	A	8	3	#	#
3	A	0	#	#	B	C	2	8	#	#	#	#	#	#	#	#	7	3	1	9	#	#	4	6	5	−
4	0	9	7	2	#	#	A	C	B	−	6	3	#	#	5	4	1	8	#	#	#	#	#	#	#	#
5	8	0	#	#	5	3	−	4	9	C	#	#	A	B	1	7	#	#	#	#	#	#	#	#	6	2
6	0	7	#	#	#	#	#	#	#	#	8	C	1	6	#	#	B	9	−	A	2	5	#	#	3	4
7	6	0	#	#	#	#	#	#	#	#	1	5	7	C	#	#	4	2	−	3	8	B	#	#	9	A
8	0	5	#	#	A	8	−	9	1	4	#	#	2	3	6	C	#	#	#	#	#	#	#	#	B	7
9	4	0	B	6	#	#	1	3	2	−	A	7	#	#	9	8	5	C	#	#	#	#	#	#	#	#
A	0	3	#	#	1	2	5	B	#	#	#	#	#	#	#	#	A	6	4	C	#	#	7	9	8	−
B	2	0	−	1	6	9	#	#	7	8	B	4	#	#	#	#	#	#	#	#	3	C	A	5	#	#
C	0	1	4	A	#	#	#	#	#	#	#	#	9	5	3	B	#	#	6	8	7	−	2	C	#	#

Kovílas Logaritmus už netrpělivě čekal, kdy se dostane ke slovu. Když se tak stalo, začal tím, že jistě dobře znají, jak se zavádí logaritmus v oboru reálných čísel. Jde o to, že z exponenciálního vztahu

$y = a^x$,

kde a je kladné číslo různé od 1, můžeme vyjádřit x jako logaritmus kladného čísla y o základu a:

$x = \log_a y$

Z pravidel o počítání s logaritmy si připomeňme, že platí

$\log_a 1 = 0;\ \log_a a = 1$

$\log_a (x.y) = \log_a x + \log_a y$

A podobně můžeme zavést "logaritmus" i mezi trettočísly . Platí-li

$y = a^x$,

kde a je primitivní kořen a x libovolné tolvočíslo, můžeme vyjádřit x jako ***diskrétní logaritmus*** (podle modulu 13)[9] nenulového čísla y o základu a:

$x = \mathrm{dlog}_a\ y$.

Jako příklad zvolme $a = 6$. Z tabulky mocnin si vyberme řádek mocnin 6 a vytvořme samostatnou tabulku mocnin 6:

x	0	1	2	3	4	5	6	7	8	9	A	B	C
6^x	1	6	A	8	9	2	C	7	3	5	4	B	1

Když vyměníme pořadí řádků, upravíme levá záhlaví a sloupce uspořádáme tak, aby se v tabulce pro jednotlivá y dobře hledaly příslušné diskrétní logaritmy, dostaneme tabulku diskrétních logaritmů:

y	1	2	3	4	5	6	7	8	9	A	B	C
$\mathrm{dlog}_6\ y$	0	5	8	A	9	1	7	3	4	2	B	6

Připomeňme, že y je nenulové trettočíslo, kdežto jeho diskrétní logaritmus tolvočíslo.

Pro diskrétní logaritmy platí podobně jako pro obyčejné logaritmy

$\mathrm{dlog}_a\ 1 = 0;\ \mathrm{dlog}_a\ a = 1$

$\mathrm{dlog}_a\ (x.y) = \mathrm{dlog}_a\ x + \mathrm{dlog}_a\ y$ (na pravé straně jde ovšem o sčítání tolvočísel).

Aby to demonstroval na příkladě, zůstal kovílas Logaritmus u základu 6 a zvolil $x = 5$, $y = 9$. Vynásobíme-li trettočísla 5 a 9, dostaneme 6. V tabulce najdeme $\mathrm{dlog}_6\ 5 = 9$, $\mathrm{dlog}_6\ 9 = 4$

[9] Někdy se používá termín index

a i bez použití tabulky víme, že $\mathrm{dlog}_6 6 = 1$. Sečteme-li diskrétní logaritmy činitelů, tedy 9 a 4 jako tolvočísla, dostaneme skutečně 1. Zatímco převedení násobení čísel na sčítání logaritmů se může velice dobře uplatnit při výpočtu, v oblasti trettočísel (a tolvočísel jako exponentů) je to jen hezká zajímavost.[10]

Čas neuvěřitelně rychle utíkal, děti se toho dověděly hodně, a tak nadešel čas pro Alguelitino závěrečné slovo. Ta je v něm pochválila za pozornost a připomněla, že se seznámily s trettočísly, jichž je jen třináct, a při tom pro operace mezi nimi platí stejné zákona jako pro operace mezi reálnými čísly. Mezi trettočísly zvláštní postavení zaujímá nula; nenulová trettočísla však nerozdělujeme na kladná a záporná. Zápornost se do pohádkové říše nehodí. Alguelita se svými spolupracovníky, vílami a kovílasy, skřítky a dalším pohádkovými bytostmi vědí, že smyslem života je společně konat dobro a usilovat o ně. Proto jim velice vyhovuje, že trettočísla nelze nějak rozumně uspořádat pomocí vztahů 'větší – menší', 'horší – lepší'. V pohádkové říši nechtějí konkurenci, jeden v druhém vidí spolupracovníka, přítele, bratra, sestru.

Jeskynní setkání ukončila slovy: "Vážím si lidmi používané struktury reálných čísel. Ale nehodí se ke všemu a někdy vede na scestí. Jejich lineární uspořádání ('větší – menší', 'horší – lepší') je užitečné pro počítání, ale týká se čísel, a nikoli živých tvorů. I ve skutečném světě je důležitá neporovnatelnost. Je krásné, když lidé mohou společně, každý podle svých schopností a možností, usilovat o dobro. Každý jsme jiný, umíme něco jiného; máme svá obdarování a vzájemně jeden potřebujeme druhého. A je skvělé, že máme jeden druhého po boku. – Vědomě používám první osobu, patřím jak světu pohádek, tak i lidskému světu, krásnému, bohatému, trpícímu rostoucím násilím a očekávajícímu rozmnožování dobra.

Doufám, že jste v naší jeskyni Třináctce prožily příjemné a ducha občerstvující chvíle, že vám bylo dobře spolu s vílami a kovílasy a i se mnou. Kéž byste se odtud vrátily obohaceny nejen matematicky, ale i všeobecně lidsky. Mějte se moc dobře a ať je i dobře všem, s nimiž se setkáte."

Literatura

1. NEČAS, J.: Vlci a zajíci v pohádkovém lese. Envigogika 2009/IV/2 (Inspirace) – Mundus Symbolicus 2009.
2. NEČAS, J.: Princezna Alguelita a rozmanitost v přírodě. Envigogika 2011/VI/1 (Inspirace)
3. PELIKÁN, J. – HENZLER, J.: Matematické základy informatiky. Praha, Oeconomica 2008.
4. ELIZAGARAY, Alga M.: Niños, Autores y Libros. La Habana, Gente Nueva 1981.

[10] Pokud bychom pracovali s podobnou strukturou, počet jejíchž prvků by místo 13 byl vyjádřen nesmírně velkým prvočíslem, nalezly by diskrétní logaritmy významné uplatnění v kryptografických metodách