Násobíme chytře?

L'ubomíra Balková

Katedra matematiky
Fakulta jaderná a fyzikálně inženýrská
České vysoké učení technické v Praze

7. března 2013

Program

1. Historické násobení
   - Indické násobení
   - Čínské násobení
   - Egyptské (etiopské) násobení
   - Ruské (sedlácké) násobení
   - Cauchyovo komplementární násobení
   - Násobení pomocí prstů
   - Kulikovo dvojciferné násobení
   - Tabulky čtvrtkvadrátů
   - Napierovy kosti
2. Počítačové násobení
   - Násobení v binární soustavě
   - Násobení v redundantní binární soustavě
   - Karacubovo násobení

- **Definice** (Ottův slovník naučný):
  Násobení v mathematice jest základní úkon početní, kterým hledáme součet dvou nebo několika čísel stejné velikosti.

- **Definice** (Ottův slovník naučný):
  Násobení v mathematice jest základní úkon početní, kterým hledáme součet dvou nebo několika čísel stejné velikosti.
- **Etymologie**: *násobeno* vzniklo z *na sobě*, tj. trojnásobný je vlastně trojí na sobě

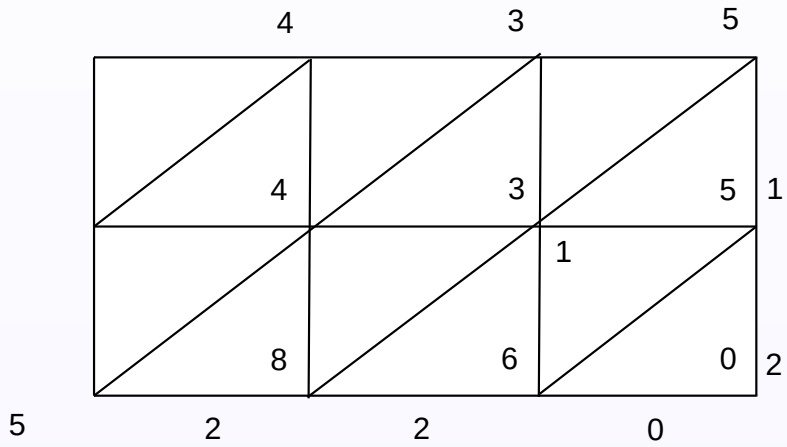
- **Definice** (Ottův slovník naučný):
  Násobení v mathematice jest základní úkon početní, kterým hledáme součet dvou nebo několika čísel stejné velikosti.
- **Etymologie**: *násobeno* vzniklo z *na sobě*, tj. trojnásobný je vlastně trojí na sobě
- $\times$ poprvé 1631 – William Oughtred *Clavis mathematicae*
  $\cdot$ poprvé 1698 – Leibnizův dopis Johannovi Bernoullimu

Program

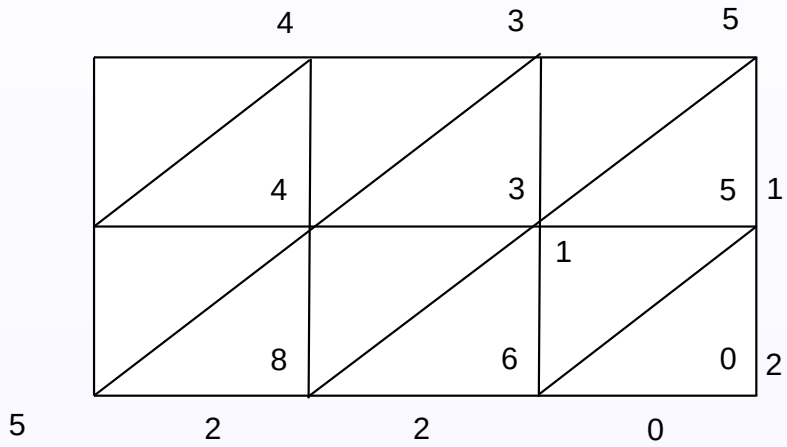
Program

- chceme násobit 435×12

- chceme násobit 435×12

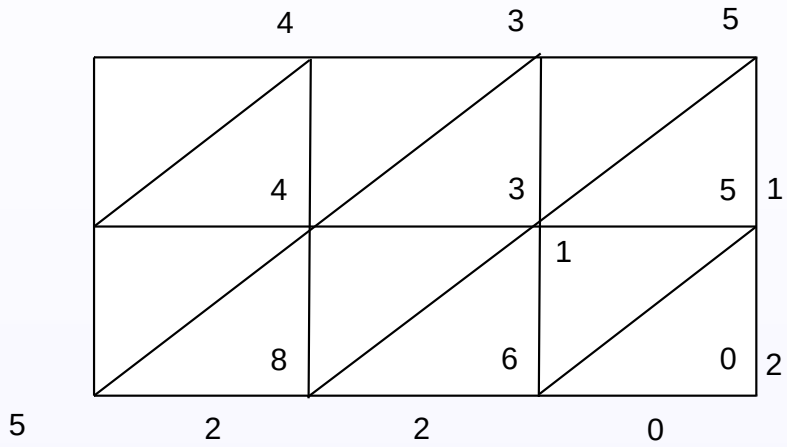


- chceme násobit 435×12



- známých je více než 8 způsobů násobení

- chceme násobit 435×12

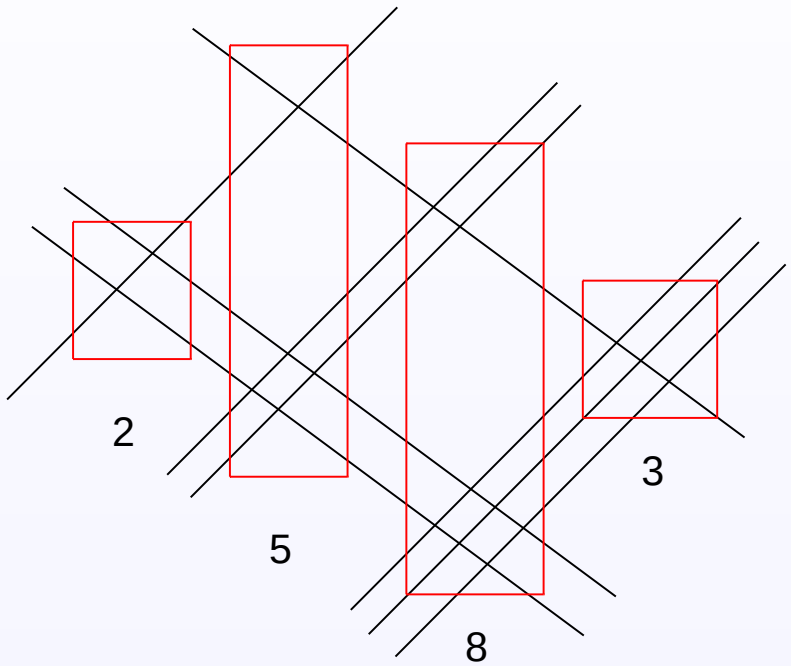


- známých je více než 8 způsobů násobení
- Leonardo Pisánský (1170-1250): "Devatero znaků indických je $1, 2, 3, 4, 5, 6, 7, 8, 9$, těmito devíti znaky a znakem 0, který se arabsky zefír nazývá, se dá zapsat každé číslo."

Program

- chceme násobit 123×21

- chceme násobit 123×21



Program

- chceme násobit 13×15

- chceme násobit 13×15

13	$\times$	15
$\sqrt{1}$		15
2		30
$\sqrt{4}$		60
$\sqrt{8}$		120
		195

- chceme násobit 13×15

13	$\times$	15
$\sqrt{1}$		15
2		30
$\sqrt{4}$		60
$\sqrt{8}$		120
		195

- původ: rovnoramenné váhy,
  uměli získávat závaží a, $2a$, $4a$, $8a$, $16a, \ldots$ a všimli si, že pomocí nich vyváží jakékoliv závaží hmotnosti $b \times a$

Program

- chceme násobit 13×15

- chceme násobit 13×15
- díváme se na zbytky po dělení 2

- chceme násobit 13×15
- díváme se na zbytky po dělení 2

13	$\times$	15
$13 : 2 = 6$	zbytek 1	15
$6 : 2 = 3$	zbytek 0	30
$3 : 2 = 1$	zbytek 1	60
$1 : 2 = 0$	zbytek 1	120
		195

- chceme násobit 13×15
- díváme se na zbytky po dělení 2

13	×	15
$13 : 2 = 6$	zbytek 1	15
$6 : 2 = 3$	zbytek 0	30
$3 : 2 = 1$	zbytek 1	60
$1 : 2 = 0$	zbytek 1	120
		195

- po zavedení indicko-arabského způsobu násobení v Evropě se na sedlácké násobení zapomnělo a s překvapením pak bylo "objeveno" v Rusku v 19. století

Program

- chceme násobit 57×17

- chceme násobit 57×17
- zapíšeme čísla pomocí cifer z $\{-4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$

- chceme násobit 57×17
- zapíšeme čísla pomocí cifer z $\{-4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$

$$57 = 1\overline{43} = 100 - 40 - 3 \quad \text{a} \quad 17 = 2\overline{3} = 20 - 3$$

- chceme násobit 57×17
- zapíšeme čísla pomocí cifer z $\{-4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$

$$57 = 1\overline{43} = 100 - 40 - 3 \quad \text{a} \quad 17 = 2\overline{3} = 20 - 3$$

	1	$\overline{4}$	$\overline{3}$
		2	$\overline{3}$
	-2	2	9
2	-8	-6	
1	0	-4	9
	9	6	9

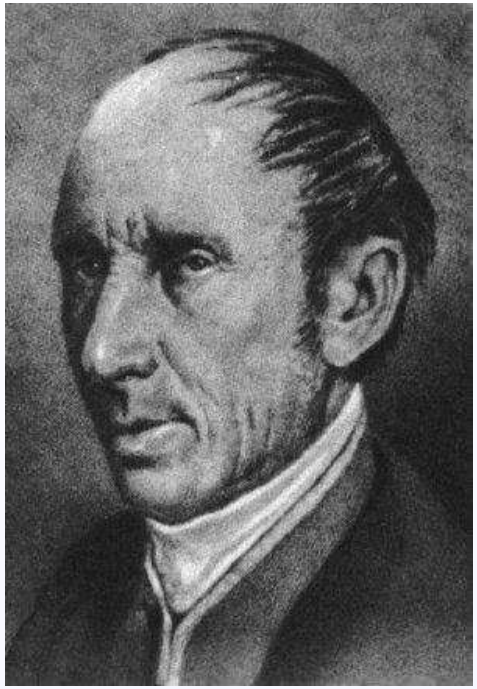
- chceme násobit 57×17
- zapíšeme čísla pomocí cifer z $\{-4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$

$$57 = 1\overline{43} = 100 - 40 - 3 \quad \text{a} \quad 17 = 2\overline{3} = 20 - 3$$

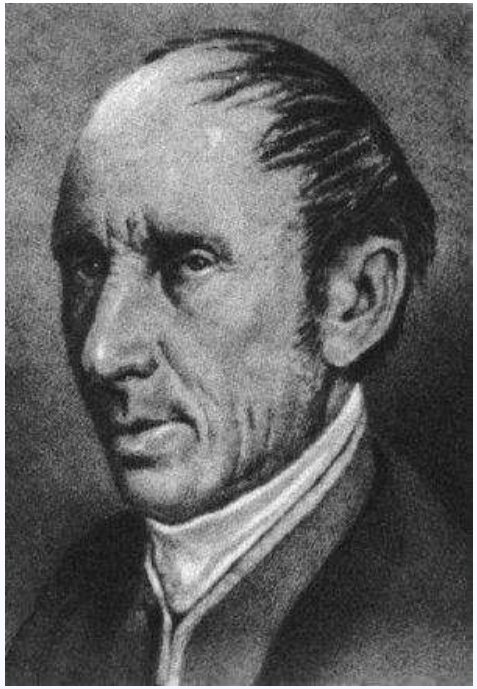
	1	$\overline{4}$	$\overline{3}$
		2	$\overline{3}$
	-2	2	9
2	-8	-6	
1	0	-4	9
	9	6	9

- vystačíme s malou násobilkou do 5×5

Augustin Louis CAUCHY (1789–1857)

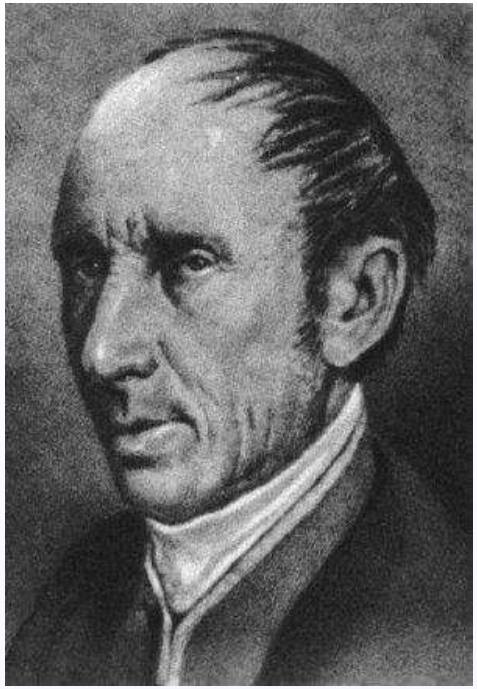


Augustin Louis CAUCHY (1789–1857)



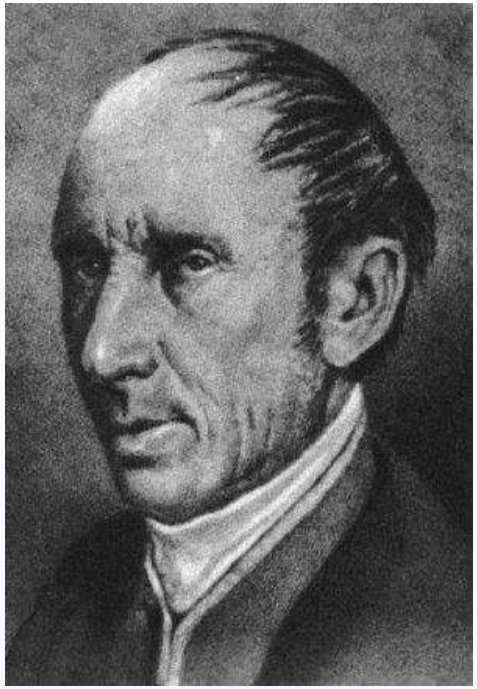
- fanatický katolík, přívrženec Bourbonů, kongregace (jezuité)

Augustin Louis CAUCHY (1789–1857)



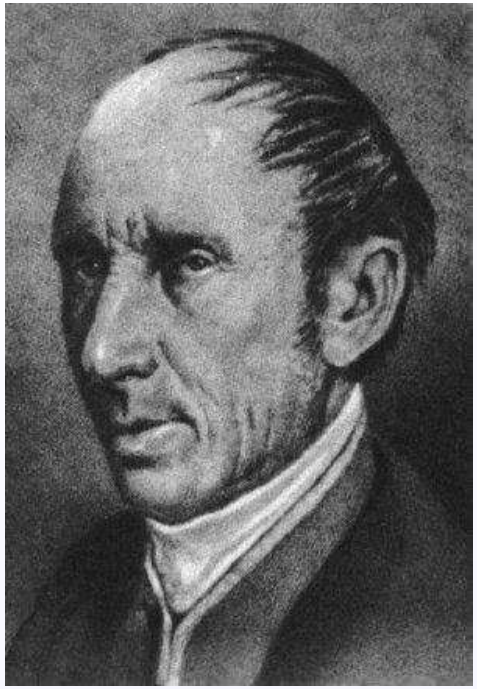
- fanatický katolík, přívrženec Bourbonů, kongregace (jezuité)
- profesor na Ecole Polytechnique - Cours d'analyse (1821): limita, spojitost, derivace, integrál, funkce komplexní proměnné, řešení diferenciálních rovnic

Augustin Louis CAUCHY (1789–1857)



- fanatický katolík, přívrženec Bourbonů, kongregace (jezuité)
- profesor na Ecole Polytechnique - Cours d'analyse (1821): limita, spojitost, derivace, integrál, funkce komplexní proměnné, řešení diferenciálních rovnic
- učitel vnuka Karla X. (pobyt v Praze 1833-35)

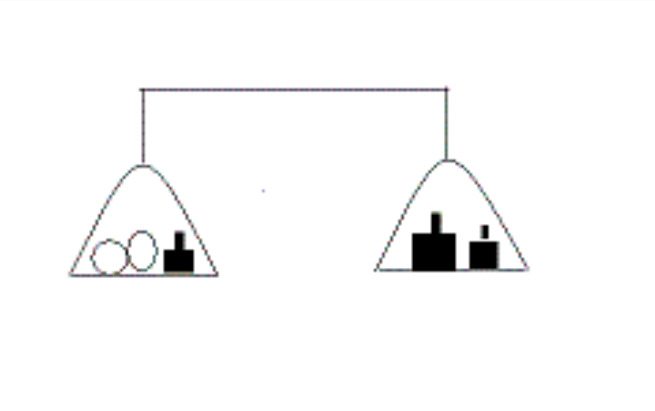
Augustin Louis CAUCHY (1789–1857)



- fanatický katolík, přívrženec Bourbonů, kongregace (jezuité)
- profesor na Ecole Polytechnique - Cours d'analyse (1821): limita, spojitost, derivace, integrál, funkce komplexní proměnné, řešení diferenciálních rovnic
- učitel vnuka Karla X. (pobyt v Praze 1833-35)
- 789 článků (více jen Erdös, Euler a Caley)

Odbočka: Balancovaná ternární soustava

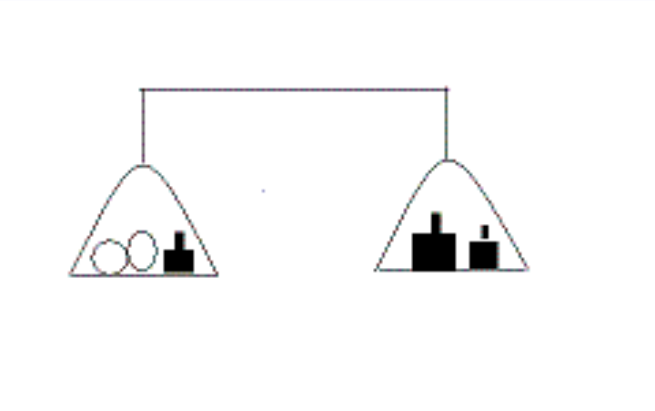
Otázka: Chceme vážit věci o hmotnostech $1, 2, \ldots, 40$ kg. Jakou nejmenší sadu závaží zvolit?



Odbočka: Balancovaná ternární soustava

Otázka: Chceme vážit věci o hmotnostech $1, 2, \ldots, 40$ kg. Jakou nejmenší sadu závaží zvolit?

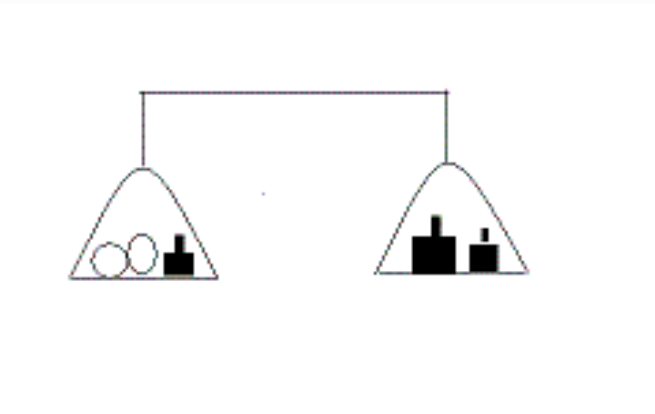
Tři závaží nestačí!



Odbočka: Balancovaná ternární soustava

Otázka: Chceme vážit věci o hmotnostech $1, 2, \ldots, 40$ kg. Jakou nejmenší sadu závaží zvolit?

Tři závaží nestačí!

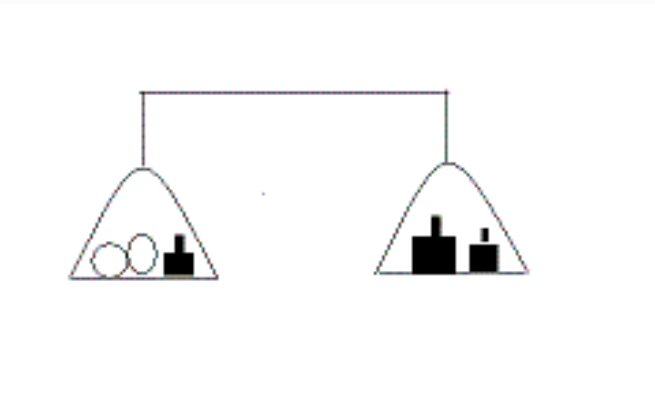


Řešení: $1, 3, 9, 27$.

Odbočka: Balancovaná ternární soustava

Otázka: Chceme vážit věci o hmotnostech $1, 2, \ldots, 40$ kg. Jakou nejmenší sadu závaží zvolit?

Tři závaží nestačí!



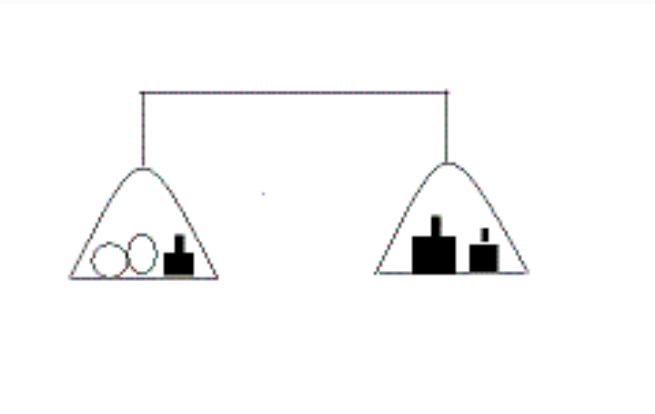
Řešení: $1, 3, 9, 27$.

$5 = 9 - 3 - 1$

Odbočka: Balancovaná ternární soustava

Otázka: Chceme vážit věci o hmotnostech $1, 2, \ldots, 40$ kg. Jakou nejmenší sadu závaží zvolit?

Tři závaží nestačí!



Řešení: $1, 3, 9, 27$.

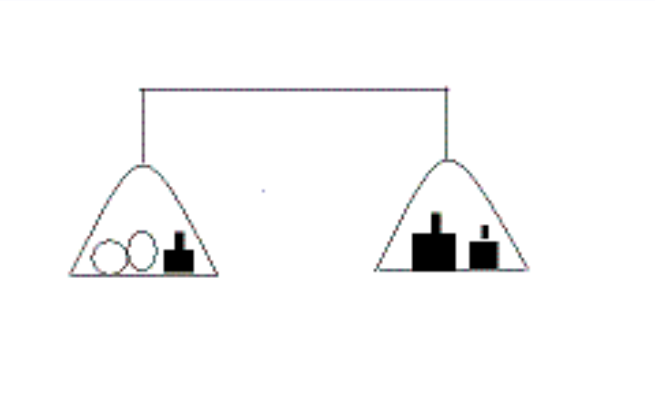
$5 = 9 - 3 - 1$

$18 = 27 - 9$

Odbočka: Balancovaná ternární soustava

Otázka: Chceme vážit věci o hmotnostech $1, 2, \ldots, 40$ kg. Jakou nejmenší sadu závaží zvolit?

Tři závaží nestačí!



Řešení: $1, 3, 9, 27$.

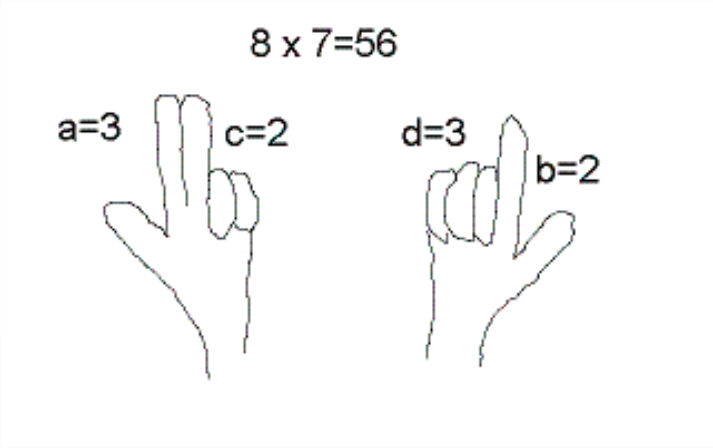
$5 = 9 - 3 - 1$
$18 = 27 - 9$

$$\{a_k 3^k + a_{k-1} 3^{k-1} + \cdots + a_1 3^1 + a_0 3^0 \mid a_i \in \{-1, 0, 1\}\} =$$
$$= \{-\tfrac{3^{k+1}-1}{2}, \ldots, 0, \ldots, \tfrac{3^{k+1}-1}{2}\}$$

Program

- cikánská násobilka – vystačíme s malou násobilkou do 5×5
- násobení devítkou

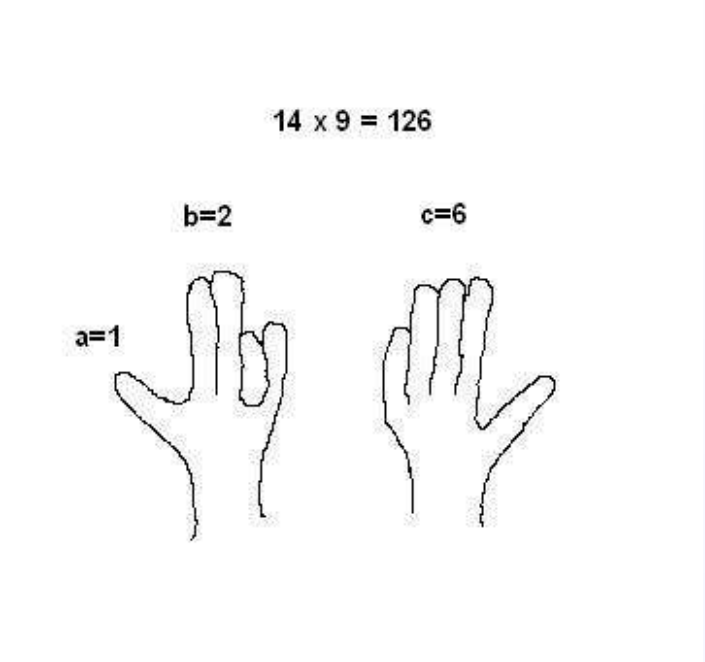
Cikánská (středověká) násobilka



- vztyčené prsty a, b
- schované prsty c, d

$$\begin{aligned}(10-c)(10-d) &= 100-(c+d)10+cd \\ &= 10(10-c-d)+cd \\ &= 10(a+b)+cd\end{aligned}$$

Násobení devítkou



- od 12 do 19 krát 9
- pro $d \in \{2, 3, \ldots, 9\}$

$$\begin{aligned}(10+d)9 &= 90+9d \\ &= 100+10(d-2)+(10-d) \\ &= 100a+10b+c\end{aligned}$$

Program

- vytvořil tabulky součinů dvojciferných čísel
- chceme násobit 1743×37

$$
\begin{array}{lllll}
43 & \times & 37 & = & 1591 \\
17 & \times & 37 & = & 629 \\
\hline
 & & & & 64491
\end{array}
$$

Program

- už staří Babyloňané znají vzorce

$$ab = \frac{1}{2}\left((a+b)^2 - a^2 - b^2\right)$$

$$ab = \frac{1}{4}\left((a+b)^2 - (a-b)^2\right)$$

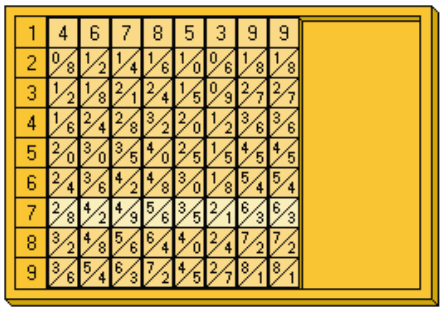
- už staří Babyloňané znají vzorce

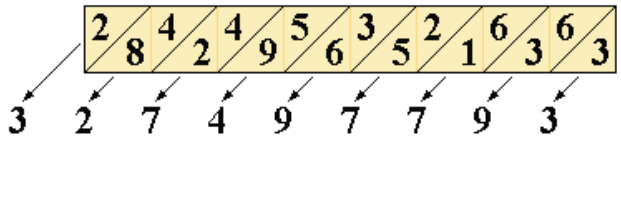
$$ab = \frac{1}{2}\left((a+b)^2 - a^2 - b^2\right)$$

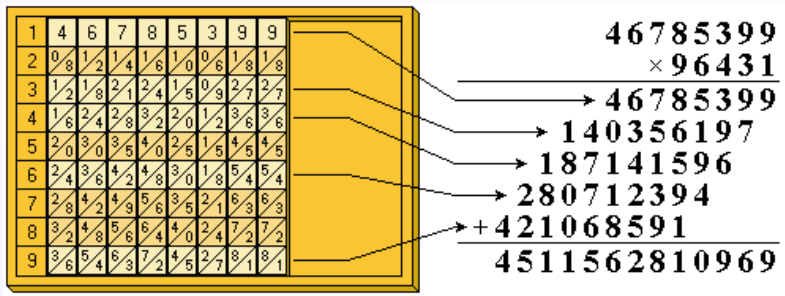
$$ab = \frac{1}{4}\left((a+b)^2 - (a-b)^2\right)$$

- 1680 – Ludolf v *Tetragonometrii* návod, jak využít tabulky čtverců k násobení
- 1816 – Anton Voisin vydává první takové multiplikační tabulky
- 1833 – Kulikovy tabulky (neví o práci svých předchůdců)

Program


1 4 6 7 8 5 3 9 9
2 0/8 1/2 1/4 1/6 1/0 0/6 1/8 1/8
3 1/2 1/8 2/1 2/4 1/5 0/9 2/7 2/7
4 1/6 2/4 2/8 3/2 2/0 1/2 3/6 3/6
5 2/0 3/0 3/5 4/0 2/5 1/5 4/5 4/5
6 2/4 3/6 4/2 4/8 3/0 1/8 5/4 5/4
7 2/8 4/2 4/9 5/6 3/5 2/1 6/3 6/3
8 3/2 4/8 5/6 6/4 4/0 2/4 7/2 7/2
9 3/6 5/4 6/3 7/2 4/5 2/7 8/1 8/1


2/8 4/2 4/9 5/6 3/5 2/1 6/3 6/3
3 2 7 4 9 7 7 9 3


1 4 6 7 8 5 3 9 9
2 0/8 1/2 1/4 1/6 1/0 0/6 1/8 1/8
3 1/2 1/8 2/1 2/4 1/5 0/9 2/7 2/7
4 1/6 2/4 2/8 3/2 2/0 1/2 3/6 3/6
5 2/0 3/0 3/5 4/0 2/5 1/5 4/5 4/5
6 2/4 3/6 4/2 4/8 3/0 1/8 5/4 5/4
7 2/8 4/2 4/9 5/6 3/5 2/1 6/3 6/3
8 3/2 4/8 5/6 6/4 4/0 2/4 7/2 7/2
9 3/6 5/4 6/3 7/2 4/5 2/7 8/1 8/1

46785399
×96431
46785399
140356197
187141596
280712394
+421068591
4511562810969

John Napier (1550 - 1617)

- fanatický protestant, teolog (na plný úvazek), matematik (ve volném čase)

John Napier (1550 - 1617)

- fanatický protestant, teolog (na plný úvazek), matematik (ve volném čase)
- objevitel logaritmů

Program

Program

- součin 11×5

$$1011 \times 101 = \begin{array}{cccccc} & & 1 & 0 & 1 & 1 \\ & & & 1 & 0 & 1 \\ \hline & & 1 & 0 & 1 & 1 \\ & 0 & 0 & 0 & 0 & \\ 1 & 0 & 1 & 1 & & \\ \hline 1 & 1 & 0 & 1 & 1 & 1 \end{array}$$

- součin 11×5

$$1011 \times 101 = \begin{array}{cccccc} & & 1 & 0 & 1 & 1 \\ & & & 1 & 0 & 1 \\ \hline & & 1 & 0 & 1 & 1 \\ & 0 & 0 & 0 & 0 & \\ 1 & 0 & 1 & 1 & & \\ \hline 1 & 1 & 0 & 1 & 1 & 1 \end{array}$$

- rychlost násobení $\sim$ počet nul v binárním zápisu násobitele

Program

- mocniny dvou $(2^k)_{k=0}^{+\infty}$ a cifry z $\{-1, 0, 1\}$

- mocniny dvou $(2^k)_{k=0}^{+\infty}$ a cifry z $\{-1, 0, 1\}$
- *redundantní*: více zápisů
  $15 = 2^3 + 2^2 + 2^1 + 2^0 = 2^4 - 2^0$,
  tedy jak 1111 tak $1000\overline{1}$ jsou zápisy 15

- mocniny dvou $(2^k)_{k=0}^{+\infty}$ a cifry z $\{-1, 0, 1\}$
- *redundantní*: více zápisů
  $15 = 2^3 + 2^2 + 2^1 + 2^0 = 2^4 - 2^0$,
  tedy jak 1111 tak $1000\overline{1}$ jsou zápisy 15
- vybereme zápis s maximálním počtem nul
  - nevyskytují se dvě nenuly vedle sebe

$$011110 \to 1000\overline{1}0 \qquad 0\overline{11110} \to \overline{1}00010$$

$$1\overline{1} \to 01 \qquad \overline{1}1 \to 0\overline{1}$$

- mocniny dvou $(2^k)_{k=0}^{+\infty}$ a cifry z $\{-1, 0, 1\}$
- *redundantní*: více zápisů
  $15 = 2^3 + 2^2 + 2^1 + 2^0 = 2^4 - 2^0$,
  tedy jak 1111 tak $1000\overline{1}$ jsou zápisy 15
- vybereme zápis s maximálním počtem nul
  - nevyskytují se dvě nenuly vedle sebe

$$011110 \to 1000\overline{1}0 \qquad 0\overline{11110} \to \overline{1}00010$$

$$1\overline{1} \to 01 \qquad \overline{1}1 \to 0\overline{1}$$

- průměrný počet nenul ve standardním binárním zápisu $= \frac{1}{2}$,
  v "minimálním" redundantním binárním zápisu $= \frac{1}{3}$

Program

- 1960 – seminář na moskevské univerzitě: Kolmogorov tvrdí, že složitost násobení dvou čísel s binárním rozvojem délky n je $\mathcal{O}(n^2)$

- 1960 – seminář na moskevské univerzitě: Kolmogorov tvrdí, že složitost násobení dvou čísel s binárním rozvojem délky n je $\mathcal{O}(n^2)$
- student Karacuba: jednoduchá myšlenka $\Rightarrow$ algoritmus násobení se složitostí $\mathcal{O}(n^{\log_2 3})$

$$\log_2 3 \doteq 1,5849 < 2$$

- následující algoritmus je podobný Karacubovu, ale jednodušší

- následující algoritmus je podobný Karacubovu, ale jednodušší
- $U = (u_{2n-1} \dots u_1 u_0)_2$ a $V = (v_{2n-1} \dots v_1 v_0)_2$

$$U = 2^n U_1 + U_0 \quad \text{a} \quad V = 2^n V_1 + V_0,$$

kde $U_1 = (u_{2n-1} \dots u_n)_2$ a $U_0 = (u_{n-1} \dots u_1 u_0)_2$,
$V_1 = (v_{2n-1} \dots v_n)_2$ a $V_0 = (v_{n-1} \dots v_1 v_0)_2$

- následující algoritmus je podobný Karacubovu, ale jednodušší
- $U = (u_{2n-1} \dots u_1 u_0)_2$ a $V = (v_{2n-1} \dots v_1 v_0)_2$

$$U = 2^n U_1 + U_0 \quad \text{a} \quad V = 2^n V_1 + V_0,$$

kde $U_1 = (u_{2n-1} \dots u_n)_2$ a $U_0 = (u_{n-1} \dots u_1 u_0)_2$,
$V_1 = (v_{2n-1} \dots v_n)_2$ a $V_0 = (v_{n-1} \dots v_1 v_0)_2$

- následující formule redukuje problém na 3 násobení n-bitových čísel a několik sčítání a posouvání binární čárky

$$UV = (2^{2n} + 2^n) U_1 V_1 + 2^n (U_1 - U_0)(V_0 - V_1) + (2^n + 1) U_0 V_0$$

- následující algoritmus je podobný Karacubovu, ale jednodušší
- $U = (u_{2n-1} \dots u_1 u_0)_2$ a $V = (v_{2n-1} \dots v_1 v_0)_2$

$$U = 2^n U_1 + U_0 \quad \text{a} \quad V = 2^n V_1 + V_0,$$

kde $U_1 = (u_{2n-1} \dots u_n)_2$ a $U_0 = (u_{n-1} \dots u_1 u_0)_2$,
$V_1 = (v_{2n-1} \dots v_n)_2$ a $V_0 = (v_{n-1} \dots v_1 v_0)_2$

- následující formule redukuje problém na 3 násobení n-bitových čísel a několik sčítání a posouvání binární čárky

$$UV = (2^{2n} + 2^n) U_1 V_1 + 2^n (U_1 - U_0)(V_0 - V_1) + (2^n + 1) U_0 V_0$$

- adaptace na decimální soustavu – násobení 8-místných čísel zpaměti

- rekurzivní proces násobení:

$$T(n) \ldots \text{složitost násobení } n\text{-bitových čísel}$$

$$T(2n) \leq 3T(n) + cn$$

- MI se ověří

$$T(2^k) \leq c(3^k - 2^k), \ k \geq 1$$

- pak platí

$$T(n) \leq T(2^{\lceil \log_2 n \rceil}) \leq c(3^{\lceil \log_2 n \rceil} - 2^{\lceil \log_2 n \rceil}) < 3c3^{\log_2 n} = 3cn^{\log_2 3}$$

Děkuji za pozornost!