Platónske telesá, polia

Algebra a diskrétna matematika

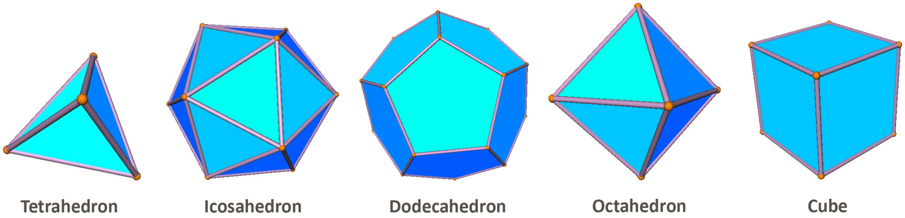
Prednáška č. 12

doc. RNDr. Jana Šiagiová, PhD.

Platónske telesá

Platónske teleso je mnohosten tvorený pravidelnými zhodnými mnohouholníkmi.

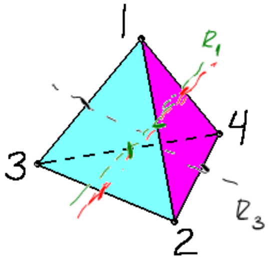
Existuje len 5 nasledujúcich platónskych telies.



štvorsten	dvadsat'sten	dvanást'sten	osemsten	kocka

Príklad

Určte grupu rotácií pravidelného štvorstena.



ROTÁCIA OKOLO OSI CEZ VRCHOL 1
A STRED PROTIĽAHLEJ STENY

ZÁPIS POMOCOU PERM.

$r_1 \to 120^\circ$ $(2\ 3\ 4)$

$r_1^2 \to 240^\circ$ $(2\ 4\ 3)$

$e \to 360^\circ$

ĎALŠIE ROTÁCIE

r_2 r_3 r_4 $(1\ 2\ 3)$

r_2^2 r_3^2 r_4^2 $(1\ 3\ 2)$

SPOLU 9

ROTÁCIE OKOLO OSÍ
CEZ STREDY PROTIĽAHLÝCH HRÁN

$R_1 \to 180^\circ \Rightarrow (12)(34)$

R_2 $(14)(23)$

R_3 $(13)(24)$

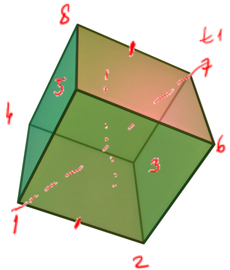
3

$= \{e, r_1, r_1^2, r_2, r_2^2, r_3, r_3^2, r_4, r_4^2, R_1, R_2, R_3\}$

$|GR_\Delta| = 12$ podgrupa S_4

Príklad

Určte grupu rotácií kocky.



OSI ROTÁCIÍ

- CEZ STREDY PROTIĽAHLÝCH STIEN

$(1234)(5678) = r_1 \to 90^\circ$, $r_1^2 \to 180^\circ$, $r_1^3 \to 270^\circ$, $e \to 360^\circ$ | r_2, r_2^2, r_2^3 | r_3, r_3^2, r_3^3

- TELESOVÉ UHLOPRIEČKY

$(245)(386)$ $t_1 \to 120^\circ$, $t_1^2 \to 240^\circ$ | t_2, t_2^2 | t_3, t_3^2 | t_4, t_4^2

- CEZ STREDY PROTIĽAHLÝCH HRÁN

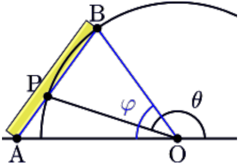
$(12)(35)(46)(78) = R_1 \to 180^\circ$, R_2, R_3, R_4, R_5, R_6

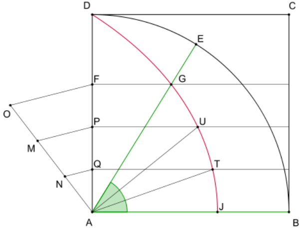
$|GR_{\square}| = 24$

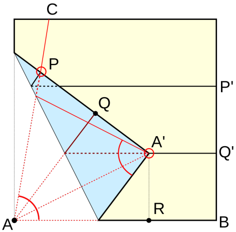
$\cong S_4$

Problém trisekcie uhla

Pomocou pravítka a kružidla zostrojte uhol, ktorý je tretinou daného uhla.

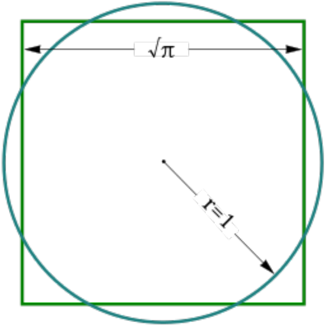


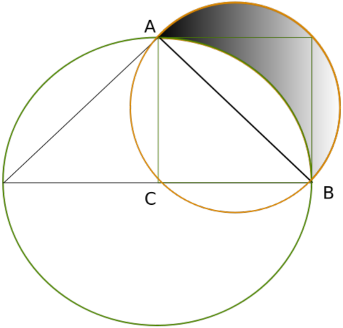




Problém kvadratúry kruhu

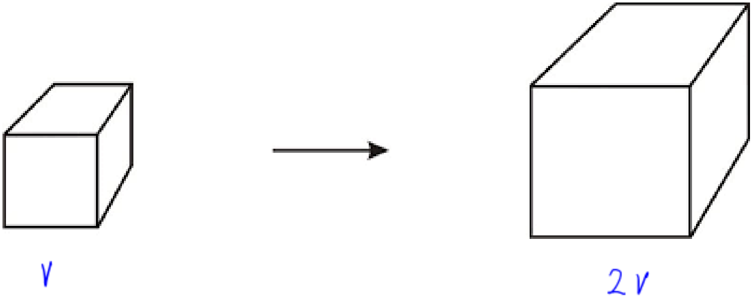
Pomocou pravítka a kružidla zostrojte štvorec, ktorý má rovnaký obsah ako daný kruh.





Problém zdvojenia kocky

Pomocou pravítka a kružidla zostrojte kocku, ktorá má dvojnásobný objem ako daná kocka.



Antické problémy

Problém trisekcie uhla, kvadratúry kruhu a zdvojenia kocky sú slávne **antické problémy**.

Úlohy sa viac ako dvetisíc rokov nedarilo vyriešiť.

Odpoveď na ne priniesla až moderná algebra v 19. storočí.

Dané problémy sú **neriešiteľné**.

Pomocou prostriedkov algebry sa dá dokázať, že pomocou pravítka a kružidla **nedokážeme** žiadnou konštrukciou

- rozdeliť daný uhol na tri rovnaké časti,
- zostrojiť z úsečky dĺžky 1 úsečku dĺžky π,
- zostrojiť z úsečky dĺžky a úsečku dĺžky $a\sqrt[3]{2}$.

Dôležitá algebraická štruktúra v tomto dôkaze je **pole**.

Pole

Pole je množina F s dvoma binárnymi operáciami $\oplus, \otimes$, pričom sú splnené nasledujúce podmienky

- $(F, \oplus)$ a $(F - \{0\}, \otimes)$ tvoria komutatívne grupy,
- Na F platí distributívny zákon
  $\forall\ a, b, c \in F: \quad a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

Operácie $\oplus, \otimes$ zvyčajne nazývame *sčitovanie* a *násobenie*.

Pole potom jednoducho zapisujeme $(F, +, \cdot)$.
Grupa $(F, +)$ sa nazýva *aditívnou* grupou poľa, skrátene F^+.

Grupa $(F - \{0\}, \cdot)$ sa nazýva *multiplikatívnou* grupou poľa, skrátene $F^\times$.

Príklad: Najznámejšie nekonečné polia

$$(\mathbb{Q}, +, \cdot) \qquad (\mathbb{R}, +, \cdot) \qquad (\mathbb{C}, +, \cdot)$$

Konečné pole - príklad 1.

Príklad konečného poľa je $(\mathbb{Z}_5, \overset{\text{mod}5}{+}, \overset{\text{mod}5}{\cdot})$.

Vypíšte všetky jeho inverzné prvky v aditínej a multiplikatívnej grupe

a riešte rovnicu $3x + 4 = 1$ v $\mathbb{Z}_5$.

$(\mathbb{Z}_5, +)$

$0 = e^+$

	INVERZ
1	$\to$ 4
2	$\to$ 3
3	$\to$ 2
4	$\to$ 1

$-1 = 4$

$-2 = 3$

$-3 = 2$

$-4 = 1$

$(\mathbb{Z}_5 - \{0\}, \cdot)$

$1 = e^{\cdot}$

	INV.
2	$\to$ 3
3	$\to$ 2
4	$\to$ 4

$2^{-1} = 3$

$3^{-1} = 2$

$4^{-1} = 4$

$3x + 4 = 1 \quad \text{mod } 5 \quad / +1$

$3x = 2 \quad / \cdot 3^{-1}$

$\cdot 2$

$\underline{\underline{x = 4}}$

V poli $(\mathbb{Z}_{11}, +, \cdot)$ riešte rovnicu

$$4x + 5 = 7 \qquad / + 6$$

$4x = 7+6 \equiv 2 \mod 11$

$4x = 2 \qquad / \cdot 4^{-1}$

$\cdot 3$

$\underline{\underline{x = 6}}$

INVERZ K 4 ?

$4 \cdot ? \equiv 1 \mod 11$

$4 \cdot 3 \equiv 1$

Príklad 3

V poli $(\mathbb{Z}_{19}, +, \cdot)$ riešte rovnicu

$$3x + 8 = 13 \quad / +11$$

$$3x = 13 + 11 \equiv 5 \quad \mathrm{mod}\ 19$$

$$3x = 5 \quad / \cdot 3^{-1}$$

$$\cdot 13$$

$$x = 5 \cdot 13$$

$$x = 65 \equiv 8 \quad \mathrm{mod}\ 19$$

$$\underline{\underline{x = 8}}$$

INVERZ K 3 ?

$$3 \cdot ? \equiv 1 \quad \mathrm{mod}\ 19$$

$$3 \cdot 13 \equiv 1$$

Príklad 4

V poli $(\mathbb{Z}_5, +, \cdot)$ riešte rovnicu

$$x^2 + 4x + 3 = 0$$

$$(x+3)(x+1) = 0$$

$$x_1 = -3 \qquad x_2 = -1$$

$$x_1 = 2 \qquad x_2 = 4$$

$D = b^2 - 4ac$ v Z_5 => $D = b^2 + a \cdot c = 4^2 + 1 \cdot 3 = 16 + 3 \equiv 4 \mod 5$

$\sqrt{D} = \sqrt{4} = 2$

$$x_{1,2} = \frac{-b \pm \sqrt{D}}{2a}$$

$x_1 = (-b + \sqrt{D}) \cdot (2a)^{-1} = (1+2) \cdot 2^{-1} = 3 \cdot 3 \equiv 4$

$x_2 = (-b - \sqrt{D}) \cdot (2a)^{-1} = (1+3) \cdot 2^{-1} = 4 \cdot 3 \equiv 2$

Príklad 5

V poli $(\mathbb{Z}_7, +, \cdot)$ riešte rovnicu

$$x^2 + 5x + 2 = 0 \quad \to \text{nemá riešenie v } Z_7$$

$D = 5^2 - 4 \cdot 1 \cdot 2 = 25 - 8 = 17 \equiv 3 \mod 7$

$\sqrt{D} = \sqrt{3} = ?$

Z_7:

x	x^2
1	1
2	4
3	2
4	2
5	4
6	1

v Z_7 majú druhú odmocninu prvky 1, 2, 4

$\sqrt{2} = 3$ $\quad\quad \sqrt{4} = 2$

$\sqrt{2} = 4$ $\quad\quad \sqrt{4} = 5$

3 nemá druhú odmocninu v Z_7

Príklad 6

V poli $(\mathbb{Z}_{11}, +, \cdot)$ riešte rovnicu

$$x^2 + 3x + 7 = 0$$

$D = 3^2 - 4 \cdot 1 \cdot 7 = 9 - 28 = -19 \equiv 3 \mod 11$

-8

$3^2 + 7 \cdot 7 = 9 + 49 = 58 \equiv 3$

$\sqrt{3} = ?$

$\sqrt{3} = 5$

$\sqrt{3} = 6$

$x_1 = (-3 + 5) \cdot 2^{-1} = 2 \cdot 6 \equiv 1$

$x_2 = (-3 + 6) \cdot 2^{-1} = 3 \cdot 6 \equiv 7$

x	x^2
1	1
2	4
3	9
4	5
5	3
6	3
7	
8	
9	
10	

$2^{-1} = ?$

$2 \cdot ? \equiv 1 \mod 11$

$2 \cdot 6 \equiv 1 \mod 11$

<u>Sk. SPR.</u>

$x = 1$

$1^2 + 3 \cdot 1 + 7 = 11 \equiv 0$

$x = 7$

$7^2 + 3 \cdot 7 + 7 = 5 + 10 + 7 \equiv 0$

V poli $\mathbb{Z}_5$ riešte sústavu rovníc

$$\begin{aligned} 3x + y &= 3 \\ x + 3y &= 2 \end{aligned}$$

$$\left(\begin{array}{cc|c} 3 & 1 & 3 \\ 1 & 3 & 2 \end{array}\right) \overset{R_1 \leftrightarrow R_2}{\sim} \left(\begin{array}{cc|c} 1 & 3 & 2 \\ 3 & 1 & 3 \end{array}\right)$$

$$\overset{R_2 + 2R_1}{\sim} \left(\begin{array}{cc|c} 1 & 3 & 2 \\ 0 & 2 & 2 \end{array}\right) \overset{R_2 : 3}{\sim} \left(\begin{array}{cc|c} 1 & 3 & 2 \\ 0 & 1 & 1 \end{array}\right) \overset{R_1 + 2R_2}{\sim} \left(\begin{array}{cc|c} 1 & 0 & 4 \\ 0 & 1 & 1 \end{array}\right)$$

$$\boxed{\begin{aligned} x &= 4 \\ y &= 1 \end{aligned}}$$

Sk. $3 \cdot 4 + 1 = 3$ ✓

$4 + 3 \cdot 1 = 2$ ✓

Príklad 8

V poli $\mathbb{Z}_7$ riešte sústavu rovníc

$$\begin{aligned} x \qquad + \; z &= 0 \\ 2x + y + 3z &= 4 \\ 5x + y + \; z &= 5 \end{aligned} \qquad \left(\begin{array}{ccc|c} 1 & 0 & 1 & 0 \\ 2 & 1 & 3 & 4 \\ 5 & 1 & 1 & 5 \end{array}\right)$$

$$\begin{array}{c} \\ R_2+R_3 \\ R_3+2R_1 \end{array} \left(\begin{array}{ccc|c} 1 & 0 & 1 & 0 \\ 0 & 2 & 4 & 2 \\ 0 & 1 & 3 & 5 \end{array}\right) \quad R_2 \leftrightarrow R_3 \left(\begin{array}{ccc|c} 1 & 0 & 1 & 0 \\ 0 & 1 & 3 & 5 \\ 0 & 2 & 4 & 2 \end{array}\right) \quad \begin{array}{c} \\ \\ R_3+5R_2 \end{array} \left(\begin{array}{ccc|c} 1 & 0 & 1 & 0 \\ 0 & 1 & 3 & 5 \\ 0 & 0 & 5 & 6 \end{array}\right)$$

$$\begin{array}{c} \\ \\ 3R_3 \end{array} \left(\begin{array}{ccc|c} 1 & 0 & 1 & 0 \\ 0 & 1 & 3 & 5 \\ 0 & 0 & 1 & 4 \end{array}\right) \quad \begin{array}{c} (R_1+6R_3) \\ R_1-R_3 \\ R_2+4R_3 \\ \\ \end{array} \left(\begin{array}{ccc|c} 1 & 0 & 0 & 3 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 4 \end{array}\right) \quad \boxed{\begin{aligned} x &= 3 \\ y &= 0 \\ z &= 4 \end{aligned}}$$

Príklad 9

V $\mathbb{Z}_6$ riešte rovnicu $3x + 4 = 2$.

$$3x + 4 = 2 \quad / + 2$$
$$3x = 4 \quad / \cdot 3^{-1}$$

$3^{-1} = ?$

$3 \cdot ? = 1 \mod 6$

$\Downarrow$

nič

K 3 neexistuje inverz mod 6

$$\boxed{\mathbb{Z}_6 \text{ NIE JE POLE}}$$

Rád poľa

Tvrdenie 1: Ak p je prvočíslo, tak pre každé $x \in \mathbb{Z}_p$ existuje prvok $y \in \mathbb{Z}_p$ taký, že $x \cdot y \equiv 1 \pmod{p}$

Rád poľa je počet prvkov poľa.

Tvrdenie 2: Rád konečného poľa je mocnina prvočísla.

Tvrdenie 3: Pre každé prvočíslo p a prirodzené číslo n existuje práve jedno (až na izomorfizmus) pole rádu $p^n = q$.

Aditívnym rádom prvku x poľa $(F, +, \cdot)$ je najmenšie prirodzené číslo n, pre ktoré platí $n \cdot x = 0$; ak také n neexistuje, rádom prvku x je ∞.

Tvrdenie 4: V každom poli majú všetky prvky rovnaký aditívny rád.

Multiplikatívnym rádom prvku x poľa $(F, +, \cdot)$ je najmenšie prirodzené číslo n, pre ktoré platí $x^n = 1$; ak také n neexistuje, rádom prvku x je ∞.

Príklad: Vypočítajte aditívny a mutliplikatívny rád prvku 2 v poli $\mathbb{Z}_{11}$.

ADITÍVNY RÁD PRVKU 2 → 11

MULTIPLIKATÍVNY RÁD PRVKU 2: → 10

$2^1 = 2$
$2^2 = 4$
$2^3 = 8$

$2^4 = 5$
$\boxed{2^5 = 10 \;\; = (-1)}$
$2^6 = 9$

VEDELI SME TU
$(-1)^2 = 1$
$(2^5)^2 = 2^{10} = 1$

$2^7 = 7$
$2^8 = 3$
$2^9 = 6$
$2^{10} = 1$

2 JE GENERÁTOR POĽA $\mathbb{Z}_{11}$

Príklad

Ktorý prvok generuje pole $\mathbb{Z}_{17}$?

$\Rightarrow$ generátor g $\Rightarrow$ $g^{16} = 1$

$\Rightarrow$ $g^{8} = -1$

SKÚSME 2

2

$2^2 = 4$

$2^3 = 8$

$2^4 = 16 = -1$

$2^8 = 1$

rád 2 je 8

nie je generátor

SKÚSME 3

3

$3^2 = 9$

$3^3 = 10$

$3^4 = 13$

$3^5 = 3 \cdot 13 = 5$

$3^6 = 3 \cdot 5 = 15$

$3^7 = 3 \cdot 15 = 11$

$3^8 = 3 \cdot 11 = 16 = -1$

$3^{16} = 1$

3 je generátor

Multiplikatívna grupa poľa

Grupa je cyklická ak je generovaná jedným prvkom.

Veta

Multiplikatívna grupa každého *konečného* poľa je **cyklická**.

Každý generátor poľa nazývame **primitívny prvok**.

Nájsť primitívny prvok v poli nie je triviálne.

Pole rádu p má $\varphi(p-1)$, kde φ je Eulerova funkcia
(počet kladných čísel menších ako $p-1$ a nesúdeliteľných s $p-1$).

Príklad: Určte počet primitívnych prvkov v poli $\mathbb{Z}_{11}$

$\varphi(11-1) = \varphi(10) = 4$

čísla < 10 nesúdeliteľné s 10 : $\{1, 3, 7, 9\}$

4 PRIMITÍVNE PRVKY V $\mathbb{Z}_{11}$

Ak prirodzené číslo n má prvočíselný rozklad $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}$, potom

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right) = n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right)$$

Príklad: Určte počet primitívnych prvkov v poliach $\mathbb{Z}_{17}, \mathbb{Z}_{19}$.

$\mathbb{Z}_{17}$: $\varphi(17-1) = \varphi(16)$ $\qquad n = 16 = 2^4$

$\varphi(16) = 16\left(1 - \frac{1}{2}\right) = 16 \cdot \frac{1}{2} = 8$

$n = 2 \cdot 9 = 2 \cdot 3^2$

$\mathbb{Z}_{19}$: $\varphi(19-1) = \varphi(18)$

$\varphi(18) = 18 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 18 \cdot \frac{1}{\cancel{2}} \cdot \frac{\cancel{2}}{3} = 6$

Príklad

Určte, ktoré prvky majú v poli $\mathbb{Z}_{19}$ druhé odmocniny.

GENERÁTOR ? $g^{18} = 1$ $g^{9} = -1$

$\sqrt{1} = 1$

2:

$\boxed{2^2 = 4} \to \sqrt{4} = 2$

$2^3 = 8$

$\boxed{2^4 = 16} \to \sqrt{16} = 2^2 = 4$

$2^5 = 13$

$\boxed{2^6 = 7} \to \sqrt{7} = 2^3 = 8$

$2^7 = 14$

$\boxed{2^8 = 9} \to \sqrt{9} = 2^4 = 16$

$2^9 = 18 = -1$ → generátor

$2^{10} = 17$ $2^{12} = 11$ $2^{14} = 6$ $2^{16} = 5$

(-2) (-8)

$\sqrt{17} = 2^5 = 13$

$\sqrt{11} = 2^6 = 7$

$\sqrt{6} = 2^7 = 14$

$\sqrt{5} = 2^8 = 9$

Príklad

$$a^{p-1} \equiv 1 \mod p$$

p - prvočíslo

Vypočítajte

$18^{18} \pmod{19} \equiv 1$

$(-1)^{18}$

$nsd(18, 19) = 1$ 19 - prvočíslo

$19669^{28} \pmod{29} \equiv 1$

$nsd(19669, 29) = 1$

29 - prvoč.

$3321^{3323} \pmod{3323} \equiv \underbrace{3321^{3322}}_{1} \cdot 3321^{1} = 3321$

prvočíslo

$nsd(3321, 3323) = 1$

Malá Fermatova veta

Nech p je prvočíslo a nech a je celé číslo nesúdeliteľné s p. Potom platí

$$a^{p-1} \equiv 1 \pmod p.$$

<u>Dôkaz:</u> Budeme dokazovať ekvivalentné tvrdenie $a^p \equiv a \pmod p$.

Matematickou indukciou vzhľadom na a, pričom p je prvočíslo a $p \nmid a$.

1. $a = 2$

$$2^p = (1+1)^p = \binom{p}{0} + \binom{p}{1} + \binom{p}{2} + \cdots + \binom{p}{p-1} + \binom{p}{p} \equiv 2 \pmod p$$

2. Predpokladajme, že platí $a^p \equiv a \pmod p$.

Ukážeme, že platí aj $(a+1)^p \equiv a+1 \pmod p$.

$$(a+1)^p = \underset{1}{\binom{p}{0}} a^p + \underbrace{\binom{p}{1} a^{p-1} + \cdots + \binom{p}{p-1} a}_{0 \bmod p} + \underset{1}{\binom{p}{p}} \equiv a^p + 1 \underset{\text{IND PREDP.}}{\equiv} a+1 \pmod p$$

Príklad

Vypočítajte

$11^{209458} \pmod{104729}$ $= 11^{2\cdot(104729)} = 11^{2\cdot 104728}\cdot 11^{2} =$

↓ prvočíslo

$= \left(11^{104728}\right)^2 \cdot 121 \equiv 121$

MFV $= 1$

nsd $(11, 104729) = 1$

$5^{243} \pmod{61}$ $= 5^{4\cdot 60+3} = \left(5^{60}\right)^4 \cdot 5^3 = 1^4 \cdot 5^3 = 125 \equiv \underline{\underline{3}}$

p = 61 - prvočíslo

MFV

1

mod 61

nsd $(5, 61) = 1$

$2021^{628132} \pmod{314067}$ $=$?

nie je prvočíslo

Veľká Fermatova veta

Pre žiadne nenulové celé čísla a, b, c a $n > 2$ neplatí

$$a^n + b^n = c^n$$

Považuje sa za jeden z najťažších matematických problémov.

V roku 1637 mal vraj Fermat jeho dôkaz.

Tvrdenie napísal na okraj Diofantovej Aritmetiky (3. st pnl). Avšak dôkaz sa mu tam už nezmestil.

Počas nasledujúcich dvoch storočí sa vedel dôkaz pre $n = 3, 5, 7$.

Prvý dôkaz publikoval v roku 1995 anglický matematik Andrew Wiles.

V tom istom roku s Richardom Taylorom odstránili medzeru v dôkaze.

K MATICI A NÁJDITE INVERZNÚ V POLI Z_7 $\quad A = \begin{pmatrix} 3 & 1 & 2 \\ 0 & 4 & 3 \\ 2 & 5 & 1 \end{pmatrix}$

$$\left(\begin{array}{ccc|ccc} 3 & 1 & 2 & 1 & 0 & 0 \\ 0 & 4 & 3 & 0 & 1 & 0 \\ 2 & 5 & 1 & 0 & 0 & 1 \end{array}\right) \begin{array}{r} 5R_1 \\ 2R_2 \\ 2R_3+R_1 \end{array} \left(\begin{array}{ccc|ccc} 1 & 5 & 3 & 5 & 0 & 0 \\ 0 & 1 & 6 & 0 & 2 & 0 \\ 0 & 4 & 4 & 1 & 0 & 2 \end{array}\right) \begin{array}{r} R_1+2R_2 \\ \\ R_3+3R_2 \end{array} \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 5 & 4 & 0 \\ 0 & 1 & 6 & 0 & 2 & 0 \\ 0 & 0 & 1 & 1 & 6 & 2 \end{array}\right)$$

$$\begin{array}{l} R_1+6R_3 \\ R_1-R_3 \\ \\ R_2+R_3 \end{array} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 4 & 5 & 5 \\ 0 & 1 & 0 & 1 & 1 & 2 \\ 0 & 0 & 1 & 1 & 6 & 2 \end{array}\right) \qquad A^{-1} = \begin{pmatrix} 4 & 5 & 5 \\ 1 & 1 & 2 \\ 1 & 6 & 2 \end{pmatrix}$$

SKÚŠKA SP.

$$\begin{pmatrix} 3 & 1 & 2 \\ 0 & 4 & 3 \\ 2 & 5 & 1 \end{pmatrix} \begin{pmatrix} 4 & 5 & 5 \\ 1 & 1 & 2 \\ 1 & 6 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Šťastné a veselé Vianoce