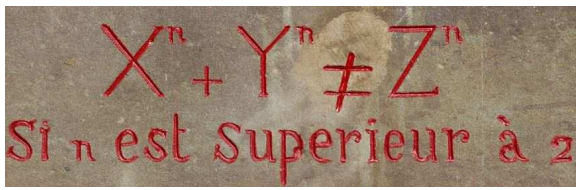
FLT – matematicky zabarvená historická exkurze

OSMA, VŠB TU, Ostrava!!!

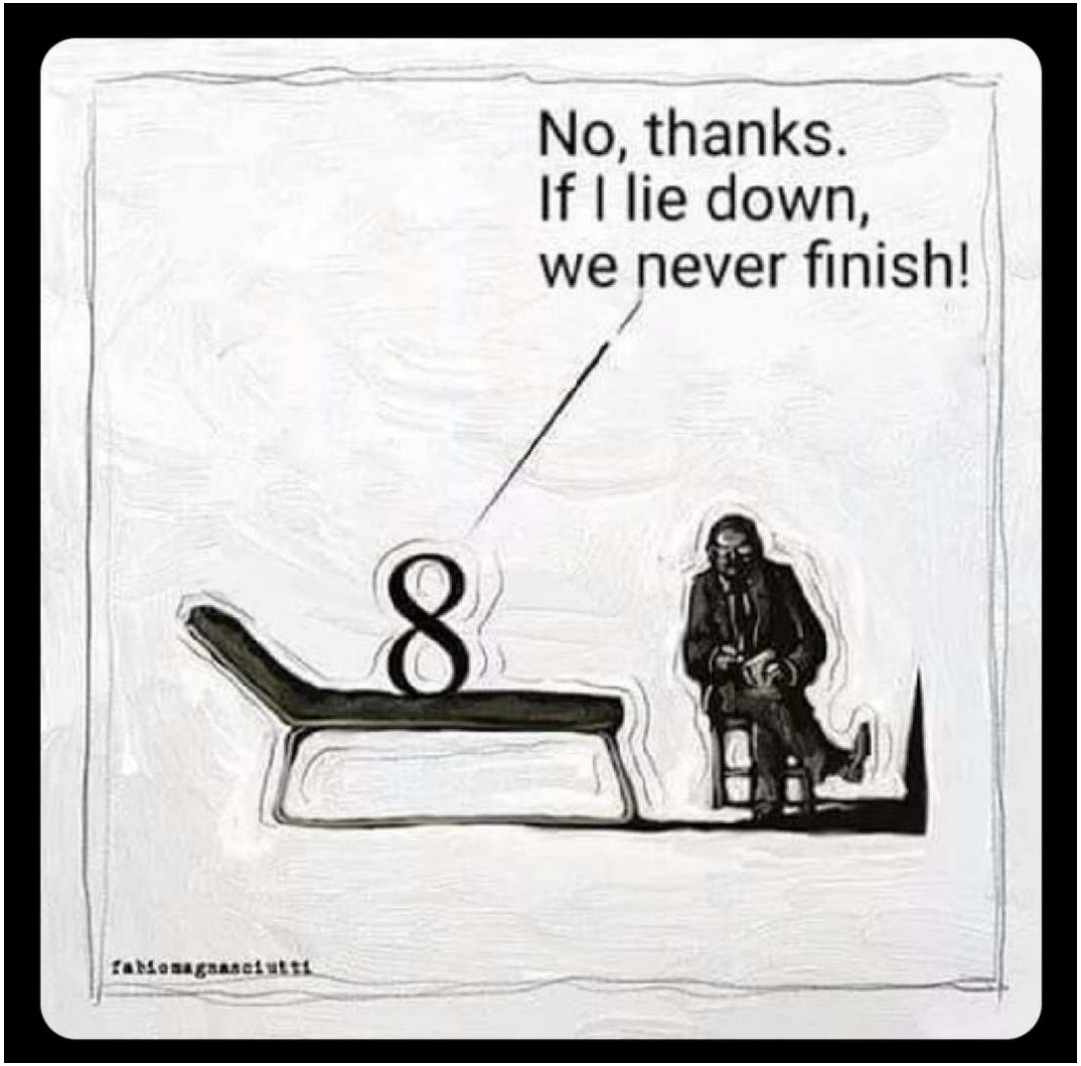
Mirko Rokyta
(8^8, aneb poosmé na Osmě, **28.3.2023**)

KMA MFF UK Praha



Věnováno OSMĚ:

Věnováno OSMĚ:



0. Úvod

Motto: Každý matematik se někdy pokusil dokázat Velkou Fermatovu větu. A pokud to popírá, snaží se o to dodnes.

(Modifikace jednoho známého výroku)

Motto: Každý matematik se někdy pokusil dokázat Velkou Fermatovu větu. A pokud to popírá, snaží se o to dodnes.

(Modifikace jednoho známého výroku)

Menu:

Motto: Každý matematik se někdy pokusil dokázat Velkou Fermatovu větu. A pokud to popírá, snaží se o to dodnes.

(Modifikace jednoho známého výroku)

Menu:

1. Jen tak na okraj

Motto: Každý matematik se někdy pokusil dokázat Velkou Fermatovu větu. A pokud to popírá, snaží se o to dodnes.

(Modifikace jednoho známého výroku)

Menu:

1. Jen tak na okraj
2. Některá triviální pozorování

Motto: Každý matematik se někdy pokusil dokázat Velkou Fermatovu větu. A pokud to popírá, snaží se o to dodnes.

(Modifikace jednoho známého výroku)

Menu:

1. Jen tak na okraj
2. Některá triviální pozorování
3. Na cestě od Fermata ke Kummerovi

Motto: Každý matematik se někdy pokusil dokázat Velkou Fermatovu větu. A pokud to popírá, snaží se o to dodnes.

(Modifikace jednoho známého výroku)

Menu:

1. Jen tak na okraj
2. Některá triviální pozorování
3. Na cestě od Fermata ke Kummerovi
4. Eliptické křivky, modulární formy a další exotická stvoření

Motto: Každý matematik se někdy pokusil dokázat Velkou Fermatovu větu. A pokud to popírá, snaží se o to dodnes.

(Modifikace jednoho známého výroku)

Menu:

1. Jen tak na okraj
2. Některá triviální pozorování
3. Na cestě od Fermata ke Kummerovi
4. Eliptické křivky, modulární formy a další exotická stvoření
5. Průlet kolem Wilesova důkazu

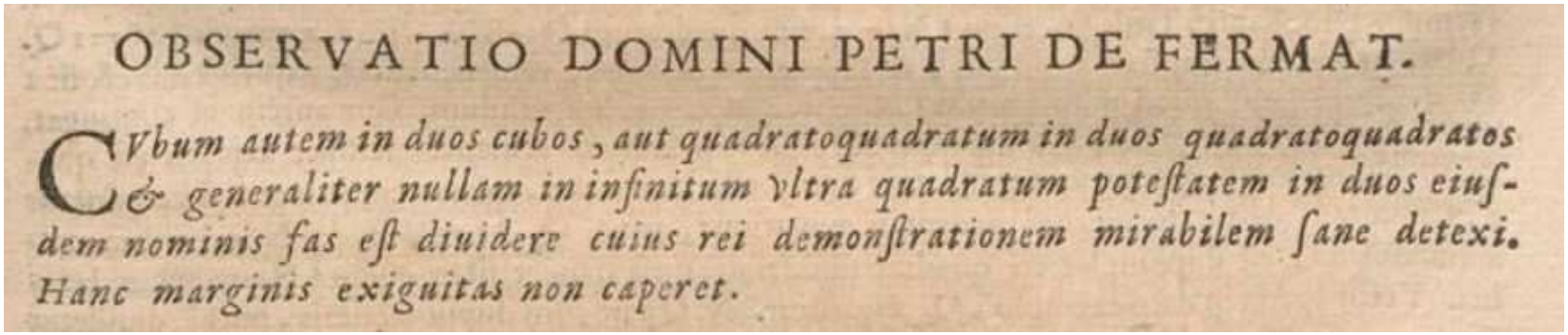
Motto: Každý matematik se někdy pokusil dokázat Velkou Fermatovu větu. A pokud to popírá, snaží se o to dodnes.

(Modifikace jednoho známého výroku)

Menu:

1. Jen tak na okraj
2. Některá triviální pozorování
3. Na cestě od Fermata ke Kummerovi
4. Eliptické křivky, modulární formy a další exotická stvoření
5. Průlet kolem Wilesova důkazu
6. Aftermath

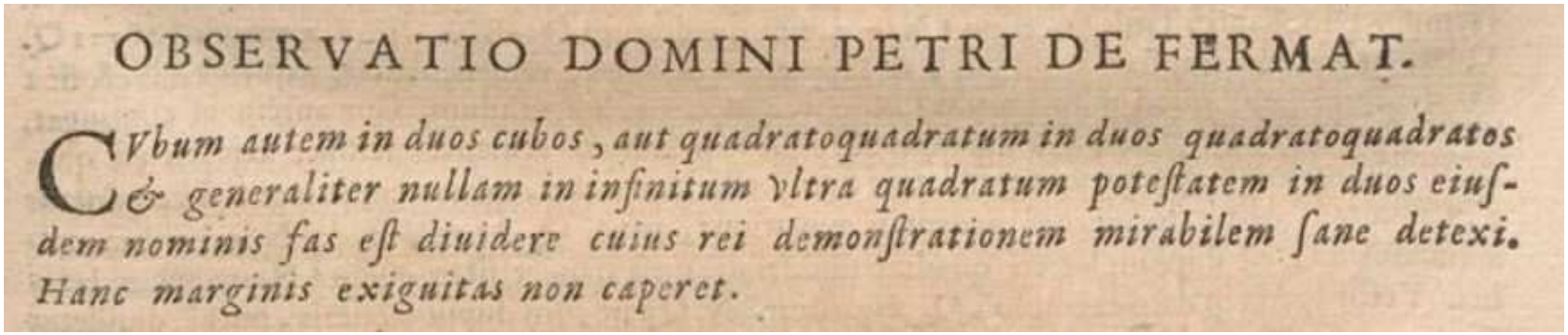
1. Jen tak na okraj



OBSERVATIO DOMINI PETRI DE FERMAT.

CVbum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum poteſtatem in duos eiuſdem nominis fas eſt diuidere cuius rei demonſtrationem mirabilem ſane detexi. Hanc marginis exiguitas non caperet.

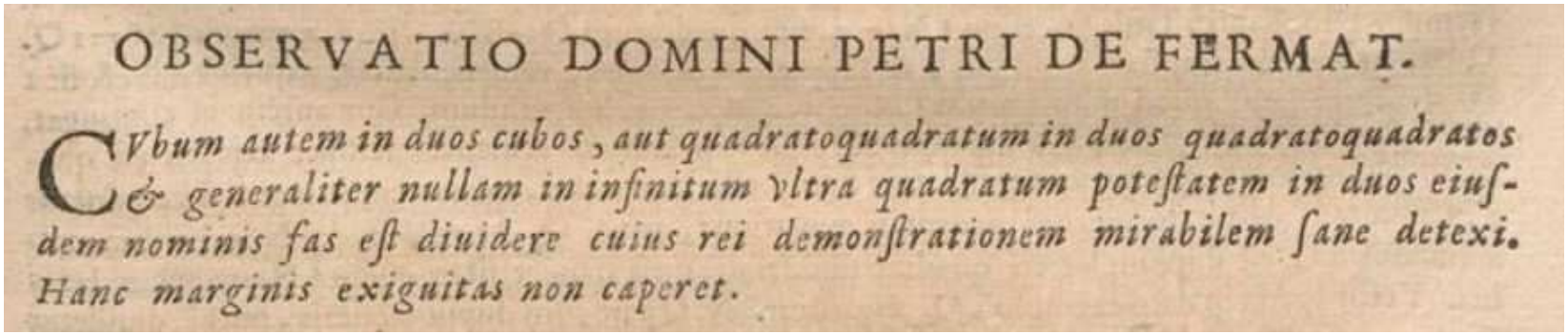
1. Jen tak na okraj



OBSERVATIO DOMINI PETRI DE FERMAT.

Cvbum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum poteſtatem in duos eiuſdem nominis fas eſt diuidere cuius rei demonſtrationem mirabilem ſane detexi. Hanc marginis exiguitas non caperet.

Krychli nelze rozdělit na dvě krychle, ani čtvrtou mocninu na dvě čtvrté mocniny, a obecně žádnou vyšší mocninu na dvě mocniny téhož stupně: objevil jsem úžasný důkaz, na který není na tomto okraji dosti místa.



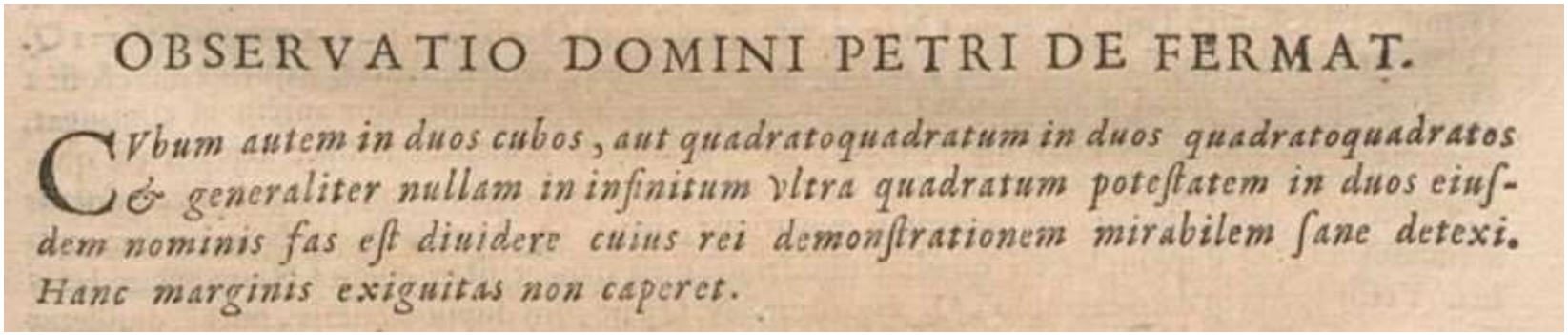
OBSERVATIO DOMINI PETRI DE FERMAT.

Cvbum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum poteſtatem in duos eiuſdem nominis fas eſt diuidere cuius rei demonſtrationem mirabilem ſane detexi. Hanc marginis exiguitas non caperet.

Krychli nelze rozdělit na dvě krychle, ani čtvrtou mocninu na dvě čtvrté mocniny, a obecně žádnou vyšší mocninu na dvě mocniny téhož stupně: objevil jsem úžasný důkaz, na který není na tomto okraji dosti místa.

Matematicky:

$$z^3 \neq x^3 + y^3 ,$$



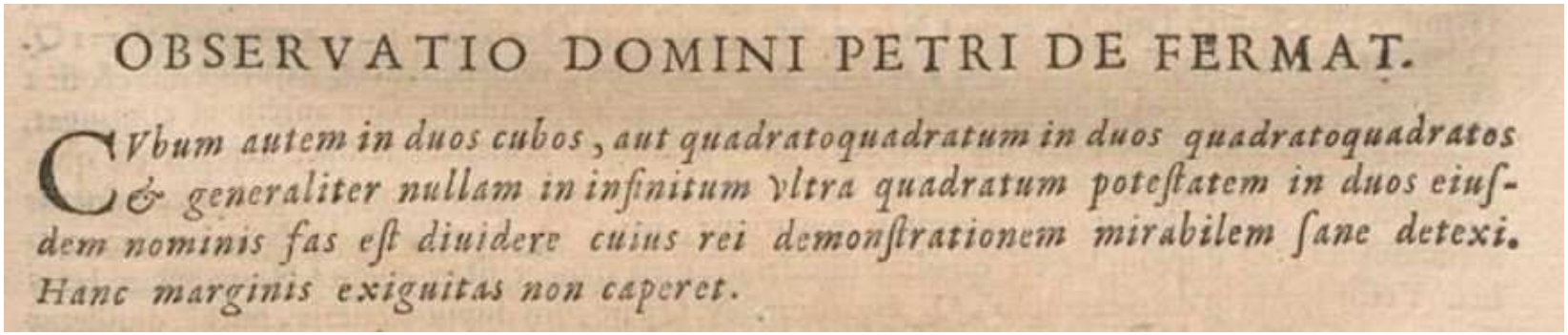
OBSERVATIO DOMINI PETRI DE FERMAT.

Cvbum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Krychli nelze rozdělit na dvě krychle, ani čtvrtou mocninu na dvě čtvrté mocniny, a obecně žádnou vyšší mocninu na dvě mocniny téhož stupně: objevil jsem úžasný důkaz, na který není na tomto okraji dosti místa.

Matematicky:

$$z^3 \neq x^3 + y^3\,, \qquad z^4 \neq x^4 + y^4\,,$$



OBSERVATIO DOMINI PETRI DE FERMAT.

Cvbum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Krychli nelze rozdělit na dvě krychle, ani čtvrtou mocninu na dvě čtvrté mocniny, a obecně žádnou vyšší mocninu na dvě mocniny téhož stupně: objevil jsem úžasný důkaz, na který není na tomto okraji dosti místa.

Matematicky:

$$z^3 \neq x^3 + y^3\,, \qquad z^4 \neq x^4 + y^4\,, \qquad \ldots \qquad z^n \neq x^n + y^n$$

Tvrzení (Pierre de Fermat, ±1637)

Jestliže n je přirozené číslo větší než 2, pak neexistují přirozená čísla x, y, z, taková, že $x^n + y^n = z^n$.

Tvrzení (Pierre de Fermat, ±1637)

Jestliže n je přirozené číslo větší než 2, pak neexistují přirozená čísla x, y, z, taková, že $x^n + y^n = z^n$.

- Spíše Poslední nerozřešená (FLT) než Velká věta.

Tvrzení (Pierre de Fermat, ±1637)

Jestliže n je přirozené číslo větší než 2, pak neexistují přirozená čísla x, y, z, taková, že $x^n + y^n = z^n$.

- Spíše Poslední nerozřešená (FLT) než Velká věta. A spíše hypotéza než věta.

Tvrzení (Pierre de Fermat, ±1637)

Jestliže n je přirozené číslo větší než 2, pak neexistují přirozená čísla x, y, z, taková, že $x^n + y^n = z^n$.

- Spíše Poslední nerozřešená (FLT) než Velká věta. A spíše hypotéza než věta. "(FLUH)"

Tvrzení (Pierre de Fermat, ±1637)

Jestliže n je přirozené číslo větší než 2, pak neexistují přirozená čísla x, y, z, taková, že $x^n + y^n = z^n$.

- Spíše Poslední nerozřešená (FLT) než Velká věta. A spíše hypotéza než věta. "(FLUH)"
- Poznámka na okraj čeho?

Tvrzení (Pierre de Fermat, ±1637)

Jestliže n je přirozené číslo větší než 2, pak neexistují přirozená čísla x, y, z, taková, že $x^n + y^n = z^n$.

- Spíše Poslední nerozřešená (FLT) než Velká věta. A spíše hypotéza než věta. "(FLUH)"
- Poznámka na okraj čeho? 2. knihy Diofantovy *Aritmetiky*

Tvrzení (Pierre de Fermat, ±1637)

Jestliže n je přirozené číslo větší než 2, pak neexistují přirozená čísla x, y, z, taková, že $x^n + y^n = z^n$.

- Spíše Poslední nerozřešená (FLT) než Velká věta. A spíše hypotéza než věta. "(FLUH)"
- Poznámka na okraj čeho? 2. knihy Diofantovy *Aritmetiky* (zachovalo se jen 6 ze 13 knih *Aritmetiky*).

Tvrzení (Pierre de Fermat, ±1637)

Jestliže n je přirozené číslo větší než 2, pak neexistují přirozená čísla x, y, z, taková, že $x^n + y^n = z^n$.

- Spíše Poslední nerozřešená (FLT) než Velká věta. A spíše hypotéza než věta. "(FLUH)"
- Poznámka na okraj čeho? 2. knihy Diofantovy *Aritmetiky* (zachovalo se jen 6 ze 13 knih *Aritmetiky*). Kniha 2, problém č. 8: ukážeme, že existuje nekonečně mnoho celočíselných řešení Pythagorovy rovnice $x^2 + y^2 = z^2$ (tzv. Pythagorejské trojice).

Tvrzení (Pierre de Fermat, ±1637)

Jestliže n je přirozené číslo větší než 2, pak neexistují přirozená čísla x, y, z, taková, že $x^n + y^n = z^n$.

- Spíše Poslední nerozřešená (FLT) než Velká věta. A spíše hypotéza než věta. "(FLUH)"
- Poznámka na okraj čeho? 2. knihy Diofantovy *Aritmetiky* (zachovalo se jen 6 ze 13 knih *Aritmetiky*). Kniha 2, problém č. 8: ukážeme, že existuje nekonečně mnoho celočíselných řešení Pythagorovy rovnice $x^2 + y^2 = z^2$ (tzv. Pythagorejské trojice). Přirozená zvídavost zřejmě Fermata vedla k tomu, aby si položil otázku co by se stalo, kdyby nahradil druhou mocninu mocninami vyššími.

1.1. Pythagorejské trojice

1.1. Pythagorejské trojice

$$1^2 \rightarrow 2^2 \rightarrow 3^2 \rightarrow 4^2 \rightarrow 5^2 \rightarrow 6^2 \rightarrow 7^2$$

1.1. Pythagorejské trojice

1^2	$\rightarrow$	2^2	$\rightarrow$	3^2	$\rightarrow$	4^2	$\rightarrow$	5^2	$\rightarrow$	6^2	$\rightarrow$	7^2
1	$\rightarrow$	4	$\rightarrow$	9	$\rightarrow$	16	$\rightarrow$	25	$\rightarrow$	36	$\rightarrow$	49

1.1. Pythagorejské trojice

1^2	$\rightarrow$	2^2	$\rightarrow$	3^2	$\rightarrow$	4^2	$\rightarrow$	5^2	$\rightarrow$	6^2	$\rightarrow$	7^2
1	$\rightarrow$	4	$\rightarrow$	9	$\rightarrow$	16	$\rightarrow$	25	$\rightarrow$	36	$\rightarrow$	49
	3		5		7		9		11		13	

1.1. Pythagorejské trojice

1^2	$\rightarrow$	2^2	$\rightarrow$	3^2	$\rightarrow$	4^2	$\rightarrow$	5^2	$\rightarrow$	6^2	$\rightarrow$	7^2
1	$\rightarrow$	4	$\rightarrow$	9	$\rightarrow$	16	$\rightarrow$	25	$\rightarrow$	36	$\rightarrow$	49
	3		5		7		9		11		13	

- Obecně $(n+1)^2 - n^2$

1.1. Pythagorejské trojice

1^2	$\rightarrow$	2^2	$\rightarrow$	3^2	$\rightarrow$	4^2	$\rightarrow$	5^2	$\rightarrow$	6^2	$\rightarrow$	7^2
1	$\rightarrow$	4	$\rightarrow$	9	$\rightarrow$	16	$\rightarrow$	25	$\rightarrow$	36	$\rightarrow$	49
	3		5		7		9		11		13	

- Obecně $(n+1)^2 - n^2 = (n^2+2n+1) - n^2$

1.1. Pythagorejské trojice

1^2	$\rightarrow$	2^2	$\rightarrow$	3^2	$\rightarrow$	4^2	$\rightarrow$	5^2	$\rightarrow$	6^2	$\rightarrow$	7^2
1	$\rightarrow$	4	$\rightarrow$	9	$\rightarrow$	16	$\rightarrow$	25	$\rightarrow$	36	$\rightarrow$	49
	3		5		7		9		11		13	

- Obecně $(n+1)^2 - n^2 = (n^2+2n+1) - n^2 = 2n+1$,

1.1. Pythagorejské trojice

1^2	$\rightarrow$	2^2	$\rightarrow$	3^2	$\rightarrow$	4^2	$\rightarrow$	5^2	$\rightarrow$	6^2	$\rightarrow$	7^2
1	$\rightarrow$	4	$\rightarrow$	9	$\rightarrow$	16	$\rightarrow$	25	$\rightarrow$	36	$\rightarrow$	49
	3		5		7		9		11		13	

- Obecně $(n+1)^2 - n^2 = (n^2+2n+1) - n^2 = 2n+1$, ve třetím řádku jsou tedy všechna lichá čísla od 3 nahoru.

1.1. Pythagorejské trojice

1^2	$\rightarrow$	2^2	$\rightarrow$	3^2	$\rightarrow$	4^2	$\rightarrow$	5^2	$\rightarrow$	6^2	$\rightarrow$	7^2
1	$\rightarrow$	4	$\rightarrow$	9	$\rightarrow$	16	$\rightarrow$	25	$\rightarrow$	36	$\rightarrow$	49
	3		5		7		9		11		13	

- Obecně $(n+1)^2 - n^2 = (n^2+2n+1) - n^2 = 2n+1$, ve třetím řádku jsou tedy všechna lichá čísla od 3 nahoru. Jsou tam tedy i všechny druhé mocniny lichých čísel

1.1. Pythagorejské trojice

1^2	$\to$	2^2	$\to$	3^2	$\to$	4^2	$\to$	5^2	$\to$	6^2	$\to$	7^2
1	$\to$	4	$\to$	9	$\to$	16	$\to$	25	$\to$	36	$\to$	49
	3		5		7		9		11		13	

- Obecně $(n+1)^2 - n^2 = (n^2+2n+1) - n^2 = 2n+1$, ve třetím řádku jsou tedy všechna lichá čísla od 3 nahoru. Jsou tam tedy i všechny druhé mocniny lichých čísel a těch je nekonečně mnoho.

1.1. Pythagorejské trojice

1^2	$\rightarrow$	2^2	$\rightarrow$	3^2	$\rightarrow$	4^2	$\rightarrow$	5^2	$\rightarrow$	6^2	$\rightarrow$	7^2
1	$\rightarrow$	4	$\rightarrow$	9	$\rightarrow$	16	$\rightarrow$	25	$\rightarrow$	36	$\rightarrow$	49
	3		5		7		9		11		13	

- Obecně $(n+1)^2 - n^2 = (n^2+2n+1) - n^2 = 2n+1$, ve třetím řádku jsou tedy všechna lichá čísla od 3 nahoru. Jsou tam tedy i všechny druhé mocniny lichých čísel a těch je nekonečně mnoho.
- Je proto nekonečně mnoho situací typu $2n + 1 = m^2$,

1.1. Pythagorejské trojice

1^2	$\to$	2^2	$\to$	3^2	$\to$	4^2	$\to$	5^2	$\to$	6^2	$\to$	7^2
1	$\to$	4	$\to$	9	$\to$	16	$\to$	25	$\to$	36	$\to$	49
	3		5		7		9		11		13	

- Obecně $(n+1)^2 - n^2 = (n^2+2n+1) - n^2 = 2n+1$, ve třetím řádku jsou tedy všechna lichá čísla od 3 nahoru. Jsou tam tedy i všechny druhé mocniny lichých čísel a těch je nekonečně mnoho.
- Je proto nekonečně mnoho situací typu $2n+1 = m^2$, pak ovšem z rovnosti

  $$n^2 + (2n+1) = (n+1)^2$$

1.1. Pythagorejské trojice

1^2	$\to$	2^2	$\to$	3^2	$\to$	4^2	$\to$	5^2	$\to$	6^2	$\to$	7^2
1	$\to$	4	$\to$	9	$\to$	16	$\to$	25	$\to$	36	$\to$	49
	3		5		7		9		11		13	

- Obecně $(n+1)^2 - n^2 = (n^2+2n+1) - n^2 = 2n+1$, ve třetím řádku jsou tedy všechna lichá čísla od 3 nahoru. Jsou tam tedy i všechny druhé mocniny lichých čísel a těch je nekonečně mnoho.
- Je proto nekonečně mnoho situací typu $2n+1 = m^2$, pak ovšem z rovnosti

  $n^2 + (2n+1) = (n+1)^2$ plyne $n^2 + m^2 = (n+1)^2$

1.1. Pythagorejské trojice

1^2	$\to$	2^2	$\to$	3^2	$\to$	4^2	$\to$	5^2	$\to$	6^2	$\to$	7^2
1	$\to$	4	$\to$	9	$\to$	16	$\to$	25	$\to$	36	$\to$	49
	3		5		7		9		11		13	

- Obecně $(n+1)^2 - n^2 = (n^2+2n+1) - n^2 = 2n+1$, ve třetím řádku jsou tedy všechna lichá čísla od 3 nahoru. Jsou tam tedy i všechny druhé mocniny lichých čísel a těch je nekonečně mnoho.
- Je proto nekonečně mnoho situací typu $2n+1 = m^2$, pak ovšem z rovnosti
  $n^2 + (2n+1) = (n+1)^2$ plyne $n^2 + m^2 = (n+1)^2$
  a tedy existuje nekonečně mnoho Pyth. trojic.

1.1. Pythagorejské trojice

1^2	$\to$	2^2	$\to$	3^2	$\to$	$\mathbf{4^2}$	$\to$	$\mathbf{5^2}$	$\to$	6^2	$\to$	7^2
1	$\to$	4	$\to$	9	$\to$	16	$\to$	25	$\to$	36	$\to$	49
	3		5		7		**9**		11		13	

- Obecně $(n+1)^2 - n^2 = (n^2+2n+1) - n^2 = 2n+1$, ve třetím řádku jsou tedy všechna lichá čísla od 3 nahoru. Jsou tam tedy i všechny druhé mocniny lichých čísel a těch je nekonečně mnoho.
- Je proto nekonečně mnoho situací typu $2n+1 = m^2$, pak ovšem z rovnosti
  $n^2 + (2n+1) = (n+1)^2$ plyne $n^2 + m^2 = (n+1)^2$
  a tedy existuje nekonečně mnoho Pyth. trojic. **Viz** ↑

1.1. Pythagorejské trojice

1^2	$\to$	2^2	$\to$	3^2	$\to$	$\mathbf{4^2}$	$\to$	$\mathbf{5^2}$	$\to$	6^2	$\to$	7^2
1	$\to$	4	$\to$	9	$\to$	16	$\to$	25	$\to$	36	$\to$	49
	3		5		7		**9**		11		13	

- Obecně $(n+1)^2 - n^2 = (n^2+2n+1) - n^2 = 2n+1$, ve třetím řádku jsou tedy všechna lichá čísla od 3 nahoru. Jsou tam tedy i všechny druhé mocniny lichých čísel a těch je nekonečně mnoho.
- Je proto nekonečně mnoho situací typu $2n+1 = m^2$, pak ovšem z rovnosti
  $n^2 + (2n+1) = (n+1)^2$ plyne $n^2 + m^2 = (n+1)^2$
  a tedy existuje nekonečně mnoho Pyth. trojic. **Viz** ↑

Pozn. Všechna řešení: $x = u^2 - v^2$, $y = 2uv$, $z = u^2 + v^2$, kde $u, v \in \mathbb{Z}$.

1.1. Pythagorejské trojice

1^2	$\to$	2^2	$\to$	3^2	$\to$	$\mathbf{4^2}$	$\to$	$\mathbf{5^2}$	$\to$	6^2	$\to$	7^2
1	$\to$	4	$\to$	9	$\to$	16	$\to$	25	$\to$	36	$\to$	49
	3		5		7		**9**		11		13	

- Obecně $(n+1)^2 - n^2 = (n^2+2n+1) - n^2 = 2n+1$, ve třetím řádku jsou tedy všechna lichá čísla od 3 nahoru. Jsou tam tedy i všechny druhé mocniny lichých čísel a těch je nekonečně mnoho.
- Je proto nekonečně mnoho situací typu $2n+1 = m^2$, pak ovšem z rovnosti
  $n^2 + (2n+1) = (n+1)^2$ plyne $n^2 + m^2 = (n+1)^2$
  a tedy existuje nekonečně mnoho Pyth. trojic. **Viz ↑**

Pozn. Všechna řešení: $x = u^2 - v^2$, $y = 2uv$, $z = u^2 + v^2$, kde $u, v \in \mathbb{Z}$. Některá řešení jsou ovšem násobky jiných.

2. Některá triviální pozorování

- **2.1. Celá nenulová nebo přirozená řešení?**

2.1. Celá nenulová nebo přirozená řešení?

Tvrzení

Následující dvě tvrzení jsou ekvivalentní:

1. *Jestliže* $n \in \mathbb{N}$, $n > 2$, *pak neexistují přirozená* x, y, z, *taková, že* $x^n + y^n = z^n$.

2.1. Celá nenulová nebo přirozená řešení?

Tvrzení

Následující dvě tvrzení jsou ekvivalentní:

1. *Jestliže* $n \in \mathbb{N}$, $n > 2$, *pak neexistují přirozená* x, y, z, *taková, že* $x^n + y^n = z^n$.
2. *Jestliže* $n \in \mathbb{N}$, $n > 2$, *pak neexistují celá nenulová* x, y, z, *taková, že* $x^n + y^n = z^n$.

2.1. Celá nenulová nebo přirozená řešení?

Tvrzení

Následující dvě tvrzení jsou ekvivalentní:

1. *Jestliže* $n \in \mathbb{N}$, $n > 2$, *pak neexistují přirozená* x, y, z, *taková, že* $x^n + y^n = z^n$.
2. *Jestliže* $n \in \mathbb{N}$, $n > 2$, *pak neexistují celá nenulová* x, y, z, *taková, že* $x^n + y^n = z^n$.

"Důkaz": pro sudá n je to jasné, pro lichá n se diskutují znaménka u x, y, z a použije se "převod záporné veličiny na druhou stranu rovnice".

2.1. Celá nenulová nebo přirozená řešení?

Tvrzení

Následující dvě tvrzení jsou ekvivalentní:

1. *Jestliže* $n \in \mathbb{N}$, $n > 2$, *pak neexistují přirozená* x, y, z, *taková, že* $x^n + y^n = z^n$.
2. *Jestliže* $n \in \mathbb{N}$, $n > 2$, *pak neexistují celá nenulová* x, y, z, *taková, že* $x^n + y^n = z^n$.

"Důkaz": pro sudá n je to jasné, pro lichá n se diskutují znaménka u x, y, z a použije se "převod záporné veličiny na druhou stranu rovnice". Ve (2) lze psát i $x^n + y^n + z^n = 0$.

2.2. Primitivní řešení

■ 2.2. Primitivní řešení

Nechť $x, y, z, n \in \mathbb{N}$, $n \geq 2$ řeší rovnici $x^n + y^n = z^n$.

2.2. Primitivní řešení

Nechť $x, y, z, n \in \mathbb{N}$, $n \geq 2$ řeší rovnici $x^n + y^n = z^n$. Pokud má některá dvojice (x, y, z) společného dělitele $d \in \mathbb{N}$, dělí d díky rovnosti $x^n + y^n = z^n$ i třetí z čísel x, y, z.

2.2. Primitivní řešení

Nechť $x, y, z, n \in \mathbb{N}$, $n \geq 2$ řeší rovnici $x^n + y^n = z^n$. Pokud má některá dvojice (x, y, z) společného dělitele $d \in \mathbb{N}$, dělí d díky rovnosti $x^n + y^n = z^n$ i třetí z čísel x, y, z. Lze tedy psát

$$x = ad, \quad y = bd, \quad z = cd, \qquad a, b, c \in \mathbb{N},$$

2.2. Primitivní řešení

Nechť $x, y, z, n \in \mathbb{N}$, $n \geq 2$ řeší rovnici $x^n + y^n = z^n$. Pokud má některá dvojice (x, y, z) společného dělitele $d \in \mathbb{N}$, dělí d díky rovnosti $x^n + y^n = z^n$ i třetí z čísel x, y, z. Lze tedy psát

$$x = ad, \quad y = bd, \quad z = cd, \qquad a, b, c \in \mathbb{N},$$

rovnost $x^n + y^n = z^n$ přejde v $(ad)^n + (bd)^n = (cd)^n$

2.2. Primitivní řešení

Nechť $x, y, z, n \in \mathbb{N}$, $n \geq 2$ řeší rovnici $x^n + y^n = z^n$. Pokud má některá dvojice (x, y, z) společného dělitele $d \in \mathbb{N}$, dělí d díky rovnosti $x^n + y^n = z^n$ i třetí z čísel x, y, z. Lze tedy psát

$$x = ad, \quad y = bd, \quad z = cd, \qquad a, b, c \in \mathbb{N},$$

rovnost $x^n + y^n = z^n$ přejde v $(ad)^n + (bd)^n = (cd)^n$ a lze ji dělit d^n.

2.2. Primitivní řešení

Nechť $x, y, z, n \in \mathbb{N}$, $n \geq 2$ řeší rovnici $x^n + y^n = z^n$. Pokud má některá dvojice (x, y, z) společného dělitele $d \in \mathbb{N}$, dělí d díky rovnosti $x^n + y^n = z^n$ i třetí z čísel x, y, z. Lze tedy psát

$$x = ad, \quad y = bd, \quad z = cd, \qquad a, b, c \in \mathbb{N},$$

rovnost $x^n + y^n = z^n$ přejde v $(ad)^n + (bd)^n = (cd)^n$ a lze ji dělit d^n. Tento proces lze opakovat, dokud nedostaneme po dvou nesoudělná čísla x, y, z, splňující $x^n + y^n = z^n$.

2.2. Primitivní řešení

Nechť $x, y, z, n \in \mathbb{N}$, $n \geq 2$ řeší rovnici $x^n + y^n = z^n$. Pokud má některá dvojice (x, y, z) společného dělitele $d \in \mathbb{N}$, dělí d díky rovnosti $x^n + y^n = z^n$ i třetí z čísel x, y, z. Lze tedy psát

$$x = ad, \quad y = bd, \quad z = cd, \qquad a, b, c \in \mathbb{N},$$

rovnost $x^n + y^n = z^n$ přejde v $(ad)^n + (bd)^n = (cd)^n$ a lze ji dělit d^n. Tento proces lze opakovat, dokud nedostaneme po dvou nesoudělná čísla x, y, z, splňující $x^n + y^n = z^n$.

Závěr.

2.2. Primitivní řešení

Nechť $x, y, z, n \in \mathbb{N}$, $n \geq 2$ řeší rovnici $x^n + y^n = z^n$. Pokud má některá dvojice (x, y, z) společného dělitele $d \in \mathbb{N}$, dělí d díky rovnosti $x^n + y^n = z^n$ i třetí z čísel x, y, z. Lze tedy psát

$$x = ad, \quad y = bd, \quad z = cd, \qquad a, b, c \in \mathbb{N},$$

rovnost $x^n + y^n = z^n$ přejde v $(ad)^n + (bd)^n = (cd)^n$ a lze ji dělit d^n. Tento proces lze opakovat, dokud nedostaneme po dvou nesoudělná čísla x, y, z, splňující $x^n + y^n = z^n$.

Závěr. BÚNO:

2.2. Primitivní řešení

Nechť $x, y, z, n \in \mathbb{N}$, $n \geq 2$ řeší rovnici $x^n + y^n = z^n$. Pokud má některá dvojice (x, y, z) společného dělitele $d \in \mathbb{N}$, dělí d díky rovnosti $x^n + y^n = z^n$ i třetí z čísel x, y, z. Lze tedy psát

$$x = ad, \quad y = bd, \quad z = cd, \qquad a, b, c \in \mathbb{N},$$

rovnost $x^n + y^n = z^n$ přejde v $(ad)^n + (bd)^n = (cd)^n$ a lze ji dělit d^n. Tento proces lze opakovat, dokud nedostaneme po dvou nesoudělná čísla x, y, z, splňující $x^n + y^n = z^n$.

Závěr. BÚNO: pro dané $n \geq 2$ hledáme $x, y, z \in \mathbb{N}$, po dvou nesoudělná řešení rovnice $x^n + y^n = z^n$.

2.2. Primitivní řešení

Nechť $x, y, z, n \in \mathbb{N}$, $n \geq 2$ řeší rovnici $x^n + y^n = z^n$. Pokud má některá dvojice (x, y, z) společného dělitele $d \in \mathbb{N}$, dělí d díky rovnosti $x^n + y^n = z^n$ i třetí z čísel x, y, z. Lze tedy psát

$$x = ad, \quad y = bd, \quad z = cd, \qquad a, b, c \in \mathbb{N},$$

rovnost $x^n + y^n = z^n$ přejde v $(ad)^n + (bd)^n = (cd)^n$ a lze ji dělit d^n. Tento proces lze opakovat, dokud nedostaneme po dvou nesoudělná čísla x, y, z, splňující $x^n + y^n = z^n$.

Závěr. BÚNO: pro dané $n \geq 2$ hledáme $x, y, z \in \mathbb{N}$, po dvou nesoudělná řešení rovnice $x^n + y^n = z^n$. Takové řešení (trojici x, y, z) Fermatovy rovnice $x^n + y^n = z^n$ nazvu jejím **primitivním řešením**.

2.2. Primitivní řešení

Nechť $x, y, z, n \in \mathbb{N}$, $n \geq 2$ řeší rovnici $x^n + y^n = z^n$. Pokud má některá dvojice (x, y, z) společného dělitele $d \in \mathbb{N}$, dělí d díky rovnosti $x^n + y^n = z^n$ i třetí z čísel x, y, z. Lze tedy psát

$$x = ad, \quad y = bd, \quad z = cd, \qquad a, b, c \in \mathbb{N},$$

rovnost $x^n + y^n = z^n$ přejde v $(ad)^n + (bd)^n = (cd)^n$ a lze ji dělit d^n. Tento proces lze opakovat, dokud nedostaneme po dvou nesoudělná čísla x, y, z, splňující $x^n + y^n = z^n$.

Závěr. BÚNO: pro dané $n \geq 2$ hledáme $x, y, z \in \mathbb{N}$, po dvou nesoudělná řešení rovnice $x^n + y^n = z^n$. Takové řešení (trojici x, y, z) Fermatovy rovnice $x^n + y^n = z^n$ nazvu jejím **primitivním řešením**. Všechna další řešení lze dostat přenásobením primitivního řešení jakýmkoli přirozeným číslem.

2.3. Parita primitivních řešení

2.3. Parita primitivních řešení

Z možných osmi možností parity (sudost=S, lichost=L) obecně nemohou pro (x, y, z) nastat situace

2.3. Parita primitivních řešení

Z možných osmi možností parity (sudost=S, lichost=L) obecně nemohou pro (x, y, z) nastat situace (L,L,L),

2.3. Parita primitivních řešení

Z možných osmi možností parity (sudost=S, lichost=L) obecně nemohou pro (x, y, z) nastat situace (L,L,L), (L,S,S),

2.3. Parita primitivních řešení

Z možných osmi možností parity (sudost=S, lichost=L) obecně nemohou pro (x, y, z) nastat situace (L,L,L), (L,S,S), (S,L,S),

2.3. Parita primitivních řešení

Z možných osmi možností parity (sudost=S, lichost=L) obecně nemohou pro (x, y, z) nastat situace (L,L,L), (L,S,S), (S,L,S), (S,S,L).

2.3. Parita primitivních řešení

Z možných osmi možností parity (sudost=S, lichost=L) obecně nemohou pro (x, y, z) nastat situace (L,L,L), (L,S,S), (S,L,S), (S,S,L). Situace (S,S,S) nedává primitivní řešení.

2.3. Parita primitivních řešení

Z možných osmi možností parity (sudost=S, lichost=L) obecně nemohou pro (x, y, z) nastat situace (L,L,L), (L,S,S), (S,L,S), (S,S,L). Situace (S,S,S) nedává primitivní řešení. Zbývající možnosti:

2.3. Parita primitivních řešení

Z možných osmi možností parity (sudost=S, lichost=L) obecně nemohou pro (x, y, z) nastat situace (L,L,L), (L,S,S), (S,L,S), (S,S,L). Situace (S,S,S) nedává primitivní řešení. Zbývající možnosti:

x	y	z	Ano/Ne	Pozn.
L	S	L		

2.3. Parita primitivních řešení

Z možných osmi možností parity (sudost=S, lichost=L) obecně nemohou pro (x, y, z) nastat situace (L,L,L), (L,S,S), (S,L,S), (S,S,L). Situace (S,S,S) nedává primitivní řešení. Zbývající možnosti:

x	y	z	Ano/Ne	Pozn.
L	S	L	Ano	

2.3. Parita primitivních řešení

Z možných osmi možností parity (sudost=S, lichost=L) obecně nemohou pro (x, y, z) nastat situace (L,L,L), (L,S,S), (S,L,S), (S,S,L). Situace (S,S,S) nedává primitivní řešení. Zbývající možnosti:

x	y	z	Ano/Ne	Pozn.
L	S	L	Ano	pro $n \geq 2$

2.3. Parita primitivních řešení

Z možných osmi možností parity (sudost=S, lichost=L) obecně nemohou pro (x, y, z) nastat situace (L,L,L), (L,S,S), (S,L,S), (S,S,L). Situace (S,S,S) nedává primitivní řešení. Zbývající možnosti:

x	y	z	Ano/Ne	Pozn.
L	S	L	Ano	pro $n \geq 2$
S	L	L		

2.3. Parita primitivních řešení

Z možných osmi možností parity (sudost=S, lichost=L) obecně nemohou pro (x, y, z) nastat situace (L,L,L), (L,S,S), (S,L,S), (S,S,L). Situace (S,S,S) nedává primitivní řešení. Zbývající možnosti:

x	y	z	Ano/Ne	Pozn.
L	S	L	Ano	pro $n \geq 2$
S	L	L	Ano	

2.3. Parita primitivních řešení

Z možných osmi možností parity (sudost=S, lichost=L) obecně nemohou pro (x, y, z) nastat situace (L,L,L), (L,S,S), (S,L,S), (S,S,L). Situace (S,S,S) nedává primitivní řešení. Zbývající možnosti:

x	y	z	Ano/Ne	Pozn.
L	S	L	Ano	pro $n \geq 2$
S	L	L	Ano	pro $n \geq 2$

2.3. Parita primitivních řešení

Z možných osmi možností parity (sudost=S, lichost=L) obecně nemohou pro (x, y, z) nastat situace (L,L,L), (L,S,S), (S,L,S), (S,S,L). Situace (S,S,S) nedává primitivní řešení. Zbývající možnosti:

x	y	z	Ano/Ne	Pozn.
L	S	L	Ano	pro $n \geq 2$
S	L	L	Ano	pro $n \geq 2$
L	L	S		

2.3. Parita primitivních řešení

Z možných osmi možností parity (sudost=S, lichost=L) obecně nemohou pro (x, y, z) nastat situace (L,L,L), (L,S,S), (S,L,S), (S,S,L). Situace (S,S,S) nedává primitivní řešení. Zbývající možnosti:

x	y	z	Ano/Ne	Pozn.
L	S	L	Ano	pro $n \geq 2$
S	L	L	Ano	pro $n \geq 2$
L	L	S	Ano	

2.3. Parita primitivních řešení

Z možných osmi možností parity (sudost=S, lichost=L) obecně nemohou pro (x, y, z) nastat situace (L,L,L), (L,S,S), (S,L,S), (S,S,L). Situace (S,S,S) nedává primitivní řešení. Zbývající možnosti:

x	y	z	Ano/Ne	Pozn.
L	S	L	Ano	pro $n \geq 2$
S	L	L	Ano	pro $n \geq 2$
L	L	S	Ano	pro $n \geq 3$ *)

2.3. Parita primitivních řešení

Z možných osmi možností parity (sudost=S, lichost=L) obecně nemohou pro (x, y, z) nastat situace (L,L,L), (L,S,S), (S,L,S), (S,S,L). Situace (S,S,S) nedává primitivní řešení. Zbývající možnosti:

x	y	z	Ano/Ne	Pozn.
L	S	L	Ano	pro $n \geq 2$
S	L	L	Ano	pro $n \geq 2$
L	L	S	Ano	pro $n \geq 3$ *)

*):

2.3. Parita primitivních řešení

Z možných osmi možností parity (sudost=S, lichost=L) obecně nemohou pro (x, y, z) nastat situace (L,L,L), (L,S,S), (S,L,S), (S,S,L). Situace (S,S,S) nedává primitivní řešení. Zbývající možnosti:

x	y	z	Ano/Ne	Pozn.
L	S	L	Ano	pro $n \geq 2$
S	L	L	Ano	pro $n \geq 2$
L	L	S	Ano	pro $n \geq 3$ *)

*): $(2k+1)^2$

2.3. Parita primitivních řešení

Z možných osmi možností parity (sudost=S, lichost=L) obecně nemohou pro (x, y, z) nastat situace (L,L,L), (L,S,S), (S,L,S), (S,S,L). Situace (S,S,S) nedává primitivní řešení. Zbývající možnosti:

x	y	z	Ano/Ne	Pozn.
L	S	L	Ano	pro $n \geq 2$
S	L	L	Ano	pro $n \geq 2$
L	L	S	Ano	pro $n \geq 3$ *)

*): $(2k+1)^2 + (2m+1)^2$

2.3. Parita primitivních řešení

Z možných osmi možností parity (sudost=S, lichost=L) obecně nemohou pro (x, y, z) nastat situace (L,L,L), (L,S,S), (S,L,S), (S,S,L). Situace (S,S,S) nedává primitivní řešení. Zbývající možnosti:

x	y	z	Ano/Ne	Pozn.
L	S	L	Ano	pro $n \geq 2$
S	L	L	Ano	pro $n \geq 2$
L	L	S	Ano	pro $n \geq 3$ *)

*): $(2k+1)^2 + (2m+1)^2 \equiv 2 \mod 4$,

2.3. Parita primitivních řešení

Z možných osmi možností parity (sudost=S, lichost=L) obecně nemohou pro (x, y, z) nastat situace (L,L,L), (L,S,S), (S,L,S), (S,S,L). Situace (S,S,S) nedává primitivní řešení. Zbývající možnosti:

x	y	z	Ano/Ne	Pozn.
L	S	L	Ano	pro $n \geq 2$
S	L	L	Ano	pro $n \geq 2$
L	L	S	Ano	pro $n \geq 3$ *)

*): $(2k+1)^2 + (2m+1)^2 \equiv 2 \mod 4, \quad (2\ell)^2$

2.3. Parita primitivních řešení

Z možných osmi možností parity (sudost=S, lichost=L) obecně nemohou pro (x, y, z) nastat situace (L,L,L), (L,S,S), (S,L,S), (S,S,L). Situace (S,S,S) nedává primitivní řešení. Zbývající možnosti:

x	y	z	Ano/Ne	Pozn.
L	S	L	Ano	pro $n \geq 2$
S	L	L	Ano	pro $n \geq 2$
L	L	S	Ano	pro $n \geq 3$ *)

*): $(2k+1)^2 + (2m+1)^2 \equiv 2 \mod 4, \quad (2\ell)^2 \equiv 0 \mod 4.$

2.3. Parita primitivních řešení

Z možných osmi možností parity (sudost=S, lichost=L) obecně nemohou pro (x, y, z) nastat situace (L,L,L), (L,S,S), (S,L,S), (S,S,L). Situace (S,S,S) nedává primitivní řešení. Zbývající možnosti:

x	y	z	Ano/Ne	Pozn.
L	S	L	Ano	pro $n \geq 2$
S	L	L	Ano	pro $n \geq 2$
L	L	S	Ano	pro $n \geq 3$ *)

*): $(2k+1)^2 + (2m+1)^2 \equiv 2 \mod 4, \quad (2\ell)^2 \equiv 0 \mod 4.$

Závěr:

2.3. Parita primitivních řešení

Z možných osmi možností parity (sudost=S, lichost=L) obecně nemohou pro (x, y, z) nastat situace (L,L,L), (L,S,S), (S,L,S), (S,S,L). Situace (S,S,S) nedává primitivní řešení. Zbývající možnosti:

x	y	z	Ano/Ne	Pozn.
L	S	L	Ano	pro $n \geq 2$
S	L	L	Ano	pro $n \geq 2$
L	L	S	Ano	pro $n \geq 3$ *)

*): $(2k+1)^2 + (2m+1)^2 \equiv 2 \mod 4, \quad (2\ell)^2 \equiv 0 \mod 4.$

Závěr: (x, y, z) je primitivním řešením Fermatovy rovnice právě tehdy, když je právě jedno z čísel x, y, z sudé.

2.3. Parita primitivních řešení

Z možných osmi možností parity (sudost=S, lichost=L) obecně nemohou pro (x, y, z) nastat situace (L,L,L), (L,S,S), (S,L,S), (S,S,L). Situace (S,S,S) nedává primitivní řešení. Zbývající možnosti:

x	y	z	Ano/Ne	Pozn.
L	S	L	Ano	pro $n \geq 2$
S	L	L	Ano	pro $n \geq 2$
L	L	S	Ano	pro $n \geq 3$ *)

*): $(2k+1)^2 + (2m+1)^2 \equiv 2 \mod 4, \quad (2\ell)^2 \equiv 0 \mod 4.$

Závěr: (x, y, z) je primitivním řešením Fermatovy rovnice právě tehdy, když je právě jedno z čísel x, y, z sudé.
V případě $n = 2$ je to právě tehdy, když je právě jedno z čísel x, y sudé.

2.4. Čtyřka a prvočíselné exponenty

2.4. Čtyřka a prvočíselné exponenty

Pokud existuje řešení (x, y, z) Fermatovy rovnice pro $n = km$,

2.4. Čtyřka a prvočíselné exponenty

Pokud existuje řešení (x, y, z) Fermatovy rovnice pro $n = km$, existuje i řešení (a, b, c) Fermatovy rovnice pro $n = m$:

2.4. Čtyřka a prvočíselné exponenty

Pokud existuje řešení (x, y, z) Fermatovy rovnice pro $n = km$, existuje i řešení (a, b, c) Fermatovy rovnice pro $n = m$:

$$x^{km} + y^{km} = z^{km}$$

2.4. Čtyřka a prvočíselné exponenty

Pokud existuje řešení (x, y, z) Fermatovy rovnice pro $n = km$, existuje i řešení (a, b, c) Fermatovy rovnice pro $n = m$:

$$x^{km} + y^{km} = z^{km} \quad \Longrightarrow \quad \underbrace{\left(x^k\right)^m}_{:=a} + \underbrace{\left(y^k\right)^m}_{:=b} = \underbrace{\left(z^k\right)^m}_{:=c}$$

2.4. Čtyřka a prvočíselné exponenty

Pokud existuje řešení (x, y, z) Fermatovy rovnice pro $n = km$, existuje i řešení (a, b, c) Fermatovy rovnice pro $n = m$:

$$x^{km} + y^{km} = z^{km} \quad \Longrightarrow \quad \underbrace{\left(x^k\right)^m}_{:=a} + \underbrace{\left(y^k\right)^m}_{:=b} = \underbrace{\left(z^k\right)^m}_{:=c}$$

jinak řečeno: pokud neexistuje řešení (a, b, c) Fermatovy rovnice (tedy pokud platí FLT) pro $n = m$,

2.4. Čtyřka a prvočíselné exponenty

Pokud existuje řešení (x, y, z) Fermatovy rovnice pro $n = km$, existuje i řešení (a, b, c) Fermatovy rovnice pro $n = m$:

$$x^{km} + y^{km} = z^{km} \quad \Longrightarrow \quad \underbrace{\left(x^k\right)^m}_{:=a} + \underbrace{\left(y^k\right)^m}_{:=b} = \underbrace{\left(z^k\right)^m}_{:=c}$$

jinak řečeno: pokud neexistuje řešení (a, b, c) Fermatovy rovnice (tedy pokud platí FLT) pro $n = m$, pak neexistuje řešení pro žádné $n = km$, $k \in \mathbb{N}$.

2.4. Čtyřka a prvočíselné exponenty

Pokud existuje řešení (x, y, z) Fermatovy rovnice pro $n = km$, existuje i řešení (a, b, c) Fermatovy rovnice pro $n = m$:

$$x^{km} + y^{km} = z^{km} \quad \Longrightarrow \quad \underbrace{\left(x^k\right)^m}_{:=a} + \underbrace{\left(y^k\right)^m}_{:=b} = \underbrace{\left(z^k\right)^m}_{:=c}$$

jinak řečeno: pokud neexistuje řešení (a, b, c) Fermatovy rovnice (tedy pokud platí FLT) pro $n = m$, pak neexistuje řešení pro žádné $n = km$, $k \in \mathbb{N}$.

Závěr:

2.4. Čtyřka a prvočíselné exponenty

Pokud existuje řešení (x, y, z) Fermatovy rovnice pro $n = km$, existuje i řešení (a, b, c) Fermatovy rovnice pro $n = m$:

$$x^{km} + y^{km} = z^{km} \quad \Longrightarrow \quad \underbrace{\left(x^k\right)^m}_{:=a} + \underbrace{\left(y^k\right)^m}_{:=b} = \underbrace{\left(z^k\right)^m}_{:=c}$$

jinak řečeno: pokud neexistuje řešení (a, b, c) Fermatovy rovnice (tedy pokud platí FLT) pro $n = m$, pak neexistuje řešení pro žádné $n = km$, $k \in \mathbb{N}$.

Závěr: Dokázat FLT (tedy dokázat, že nemá řešení pro dané n)

2.4. Čtyřka a prvočíselné exponenty

Pokud existuje řešení (x, y, z) Fermatovy rovnice pro $n = km$, existuje i řešení (a, b, c) Fermatovy rovnice pro $n = m$:

$$x^{km} + y^{km} = z^{km} \quad \Longrightarrow \quad \underbrace{\left(x^k\right)^m}_{:=a} + \underbrace{\left(y^k\right)^m}_{:=b} = \underbrace{\left(z^k\right)^m}_{:=c}$$

jinak řečeno: pokud neexistuje řešení (a, b, c) Fermatovy rovnice (tedy pokud platí FLT) pro $n = m$, pak neexistuje řešení pro žádné $n = km$, $k \in \mathbb{N}$.

Závěr: Dokázat FLT (tedy dokázat, že nemá řešení pro dané n) stačí pro $n = 4$ a všechna prvočíselná n.

3. Na cestě od Fermata ke Kummerovi

Pierre de Fermat (1601-1655)

Pierre de Fermat (1601-1655)

- Proč je královský soudce města Toulouse Pierre de Fermat považován za největšího matematika 17. století?

Pierre de Fermat (1601-1655)

- Proč je královský soudce města Toulouse Pierre de Fermat považován za největšího matematika 17. století? *Soudci měli zakázány sociální kontakty a navazování přátelství, aby nebyli v případném střetu zájmů u soudu.*

Pierre de Fermat (1601-1655)

- Proč je královský soudce města Toulouse Pierre de Fermat považován za největšího matematika 17. století? *Soudci měli zakázány sociální kontakty a navazování přátelství, aby nebyli v případném střetu zájmů u soudu.*
- Fermat nesepisoval důkazy svých tvrzení,

Pierre de Fermat (1601-1655)

- Proč je královský soudce města Toulouse Pierre de Fermat považován za největšího matematika 17. století? *Soudci měli zakázány sociální kontakty a navazování přátelství, aby nebyli v případném střetu zájmů u soudu.*
- Fermat nesepisoval důkazy svých tvrzení, typicky si dělal pouze poznámky na okrajích knih, které četl.

Pierre de Fermat (1601-1655)

- Proč je královský soudce města Toulouse Pierre de Fermat považován za největšího matematika 17. století? *Soudci měli zakázány sociální kontakty a navazování přátelství, aby nebyli v případném střetu zájmů u soudu.*
- Fermat nesepisoval důkazy svých tvrzení, typicky si dělal pouze poznámky na okrajích knih, které četl. Zachovaly se pouze náznaky několika důkazů, které jsou rekonstruovatelné a jsou v pořádku, např.:

Pierre de Fermat (1601-1655)

- Proč je královský soudce města Toulouse Pierre de Fermat považován za největšího matematika 17. století? *Soudci měli zakázány sociální kontakty a navazování přátelství, aby nebyli v případném střetu zájmů u soudu.*
- Fermat nesepisoval důkazy svých tvrzení, typicky si dělal pouze poznámky na okrajích knih, které četl. Zachovaly se pouze náznaky několika důkazů, které jsou rekonstruovatelné a jsou v pořádku, např.:
  - Číslo 26 je jediným číslem, které leží mezi druhou a třetí mocninou přirozeného čísla:

Pierre de Fermat (1601-1655)

- Proč je královský soudce města Toulouse Pierre de Fermat považován za největšího matematika 17. století? *Soudci měli zakázány sociální kontakty a navazování přátelství, aby nebyli v případném střetu zájmů u soudu.*
- Fermat nesepisoval důkazy svých tvrzení, typicky si dělal pouze poznámky na okrajích knih, které četl. Zachovaly se pouze náznaky několika důkazů, které jsou rekonstruovatelné a jsou v pořádku, např.:
  - Číslo 26 je jediným číslem, které leží mezi druhou a třetí mocninou přirozeného čísla:

$$5^2 = 25 < 26 < 27 = 3^3.$$

Pierre de Fermat (1601-1655)

- Proč je královský soudce města Toulouse Pierre de Fermat považován za největšího matematika 17. století? *Soudci měli zakázány sociální kontakty a navazování přátelství, aby nebyli v případném střetu zájmů u soudu.*
- Fermat nesepisoval důkazy svých tvrzení, typicky si dělal pouze poznámky na okrajích knih, které četl. Zachovaly se pouze náznaky několika důkazů, které jsou rekonstruovatelné a jsou v pořádku, např.:
  - Číslo 26 je jediným číslem, které leží mezi druhou a třetí mocninou přirozeného čísla:
    $$5^2 = 25 < 26 < 27 = 3^3.$$
  - Rovnice $x^n + y^n = z^n$ nemá celočíselná řešení pro $n = 4$.

Mohl mít Fermat důkaz FLT?

Mohl mít Fermat důkaz FLT?

- Fermat škodolibě trápil své současníky výzvami v dopisech, aby dokázali to, o čem on tvrdil, že umí dokázat.

Mohl mít Fermat důkaz FLT?

- Fermat škodolibě trápil své současníky výzvami v dopisech, aby dokázali to, o čem on tvrdil, že umí dokázat.
- Fermat nikdy během života nikoho nevyzval, aby FLT dokázal v plné její obecnosti,

Mohl mít Fermat důkaz FLT?

- Fermat škodolibě trápil své současníky výzvami v dopisech, aby dokázali to, o čem on tvrdil, že umí dokázat.
- Fermat nikdy během života nikoho nevyzval, aby FLT dokázal v plné její obecnosti, ani nikdy nezmínil svou slavnou poznámku na okraji.

Mohl mít Fermat důkaz FLT?

- Fermat škodolibě trápil své současníky výzvami v dopisech, aby dokázali to, o čem on tvrdil, že umí dokázat.
- Fermat nikdy během života nikoho nevyzval, aby FLT dokázal v plné její obecnosti, ani nikdy nezmínil svou slavnou poznámku na okraji.
- V "dopisech" zmiňoval jen případy $n = 4$ a $n = 3$.

Mohl mít Fermat důkaz FLT?

- Fermat škodolibě trápil své současníky výzvami v dopisech, aby dokázali to, o čem on tvrdil, že umí dokázat.
- Fermat nikdy během života nikoho nevyzval, aby FLT dokázal v plné její obecnosti, ani nikdy nezmínil svou slavnou poznámku na okraji.
- V "dopisech" zmiňoval jen případy $n = 4$ a $n = 3$.
- Slavnou poznámku na okraji našel a vydal až po Fermatově smrti jeho syn.

Mohl mít Fermat důkaz FLT?

- Fermat škodolibě trápil své současníky výzvami v dopisech, aby dokázali to, o čem on tvrdil, že umí dokázat.
- Fermat nikdy během života nikoho nevyzval, aby FLT dokázal v plné její obecnosti, ani nikdy nezmínil svou slavnou poznámku na okraji.
- V "dopisech" zmiňoval jen případy $n = 4$ a $n = 3$.
- Slavnou poznámku na okraji našel a vydal až po Fermatově smrti jeho syn.
- Fermat obecný důkaz nejspíše neměl.

Mohl mít Fermat důkaz FLT?

- Fermat škodolibě trápil své současníky výzvami v dopisech, aby dokázali to, o čem on tvrdil, že umí dokázat.
- Fermat nikdy během života nikoho nevyzval, aby FLT dokázal v plné její obecnosti, ani nikdy nezmínil svou slavnou poznámku na okraji.
- V "dopisech" zmiňoval jen případy $n = 4$ a $n = 3$.
- Slavnou poznámku na okraji našel a vydal až po Fermatově smrti jeho syn.
- Fermat obecný důkaz nejspíše neměl.

Blufoval nebo si mohl myslet, že ví, jak FLT dokázat?

Mohl mít Fermat důkaz FLT?

- Fermat škodolibě trápil své současníky výzvami v dopisech, aby dokázali to, o čem on tvrdil, že umí dokázat.
- Fermat nikdy během života nikoho nevyzval, aby FLT dokázal v plné její obecnosti, ani nikdy nezmínil svou slavnou poznámku na okraji.
- V "dopisech" zmiňoval jen případy $n = 4$ a $n = 3$.
- Slavnou poznámku na okraji našel a vydal až po Fermatově smrti jeho syn.
- Fermat obecný důkaz nejspíše neměl.

Blufoval nebo si mohl myslet, že ví, jak FLT dokázat?

Možná si myslel, že tzv. "metoda nekonečného sestupu", kterou dokázal případ $n = 4$ (a možná i $n = 3$) bude fungovat obecně.

Metoda nekonečného sestupu Pierre Fermata

Metoda nekonečného sestupu Pierre Fermata

Tvrzení (FLT pro $n = 4$)

Buďte x, y, w přirozená, že $x^4 + y^4 = w^2$. Potom existují přirozená a, b, c taková, že $a^4 + b^4 = c^2$ a $c < w$.

Metoda nekonečného sestupu Pierre Fermata

Tvrzení (FLT pro $n = 4$)

Buďte x, y, w přirozená, že $x^4 + y^4 = w^2$. Potom existují přirozená a, b, c taková, že $a^4 + b^4 = c^2$ a $c < w$.

- Jaký je tam nekonečný sestup?

Metoda nekonečného sestupu Pierre Fermata

Tvrzení (FLT pro $n = 4$)

Buďte x, y, w přirozená, že $x^4 + y^4 = w^2$. Potom existují přirozená a, b, c taková, že $a^4 + b^4 = c^2$ a $c < w$.

- Jaký je tam nekonečný sestup? Tvrzení implikuje existenci nekonečné ostře klesající posloupnosti přirozených čísel, což není možné.

Metoda nekonečného sestupu Pierre Fermata

Tvrzení (FLT pro $n = 4$)

Buďte x, y, w přirozená, že $x^4 + y^4 = w^2$. Potom existují přirozená a, b, c taková, že $a^4 + b^4 = c^2$ a $c < w$.

- Jaký je tam nekonečný sestup? Tvrzení implikuje existenci nekonečné ostře klesající posloupnosti přirozených čísel, což není možné. Tedy nemůže existovat už to první řešení.

Metoda nekonečného sestupu Pierre Fermata

Tvrzení (FLT pro $n = 4$)

Buďte x, y, w přirozená, že $x^4 + y^4 = w^2$. Potom existují přirozená a, b, c taková, že $a^4 + b^4 = c^2$ a $c < w$.

- Jaký je tam nekonečný sestup? Tvrzení implikuje existenci nekonečné ostře klesající posloupnosti přirozených čísel, což není možné. Tedy nemůže existovat už to první řešení.
- Jak z toho plyne FLT pro $n = 4$:

Metoda nekonečného sestupu Pierre Fermata

Tvrzení (FLT pro $n = 4$)

Buďte x, y, w přirozená, že $x^4 + y^4 = w^2$. Potom existují přirozená a, b, c taková, že $a^4 + b^4 = c^2$ a $c < w$.

- Jaký je tam nekonečný sestup? Tvrzení implikuje existenci nekonečné ostře klesající posloupnosti přirozených čísel, což není možné. Tedy nemůže existovat už to první řešení.
- Jak z toho plyne FLT pro $n = 4$: $x^4 + y^4 = z^4$

Metoda nekonečného sestupu Pierre Fermata

Tvrzení (FLT pro $n = 4$)

Buďte x, y, w přirozená, že $x^4 + y^4 = w^2$. Potom existují přirozená a, b, c taková, že $a^4 + b^4 = c^2$ a $c < w$.

- Jaký je tam nekonečný sestup? Tvrzení implikuje existenci nekonečné ostře klesající posloupnosti přirozených čísel, což není možné. Tedy nemůže existovat už to první řešení.
- Jak z toho plyne FLT pro $n = 4$: $x^4 + y^4 = z^4 = (z^2)^2$.

Metoda nekonečného sestupu Pierre Fermata

Tvrzení (FLT pro $n = 4$)

Buďte x, y, w přirozená, že $x^4 + y^4 = w^2$. Potom existují přirozená a, b, c taková, že $a^4 + b^4 = c^2$ a $c < w$.

- Jaký je tam nekonečný sestup? Tvrzení implikuje existenci nekonečné ostře klesající posloupnosti přirozených čísel, což není možné. Tedy nemůže existovat už to první řešení.
- Jak z toho plyne FLT pro $n = 4$: $x^4 + y^4 = z^4 = (z^2)^2$. Kdyby existovalo takové z, existuje i $w = z^2$,

Metoda nekonečného sestupu Pierre Fermata

Tvrzení (FLT pro $n = 4$)

Buďte x, y, w přirozená, že $x^4 + y^4 = w^2$. Potom existují přirozená a, b, c taková, že $a^4 + b^4 = c^2$ a $c < w$.

- Jaký je tam nekonečný sestup? Tvrzení implikuje existenci nekonečné ostře klesající posloupnosti přirozených čísel, což není možné. Tedy nemůže existovat už to první řešení.
- Jak z toho plyne FLT pro $n = 4$: $x^4 + y^4 = z^4 = (z^2)^2$. Kdyby existovalo takové z, existuje i $w = z^2$, což by bylo ve sporu s předchozím tvrzením.

Metoda nekonečného sestupu Pierre Fermata

Tvrzení (FLT pro $n = 4$)

Buďte x, y, w přirozená, že $x^4 + y^4 = w^2$. Potom existují přirozená a, b, c taková, že $a^4 + b^4 = c^2$ a $c < w$.

- Jaký je tam nekonečný sestup? Tvrzení implikuje existenci nekonečné ostře klesající posloupnosti přirozených čísel, což není možné. Tedy nemůže existovat už to první řešení.
- Jak z toho plyne FLT pro $n = 4$: $x^4 + y^4 = z^4 = (z^2)^2$. Kdyby existovalo takové z, existuje i $w = z^2$, což by bylo ve sporu s předchozím tvrzením.

Pozn: Metodou nekonečného sestupu Fermat dokázal i to, že neexistuje pravoúhlý trojúhelník s celočíselnými stranami, jehož obsah by byl čtvercem přirozeného čísla.

Leonhard Euler (1707-1783)

- Zrekonstruoval případ $n = 4$ (nekonečný sestup) z Fermatových poznámek.

Leonhard Euler (1707-1783)

- Zrekonstruoval případ $n = 4$ (nekonečný sestup) z Fermatových poznámek.
- Dokázal FLT pro $n = 3$ (1753 zmínka v dopise Goldbachovi, 1770 publikováno).

Leonhard Euler (1707-1783)

- Zrekonstruoval případ $n = 4$ (nekonečný sestup) z Fermatových poznámek.
- Dokázal FLT pro $n = 3$ (1753 zmínka v dopise Goldbachovi, 1770 publikováno). Použil ideu metody nekonečného sestupu, vyžadující ovšem sofistikovanější technické postupy.

Leonhard Euler (1707-1783)

- Zrekonstruoval případ $n = 4$ (nekonečný sestup) z Fermatových poznámek.
- Dokázal FLT pro $n = 3$ (1753 zmínka v dopise Goldbachovi, 1770 publikováno). Použil ideu metody nekonečného sestupu, vyžadující ovšem sofistikovanější technické postupy.
- Byl nesvůj z toho, že neví, jak to dokázat obecně. ("*Prohledejte pořádně Fermatovu pozůstalost!*".)

Leonhard Euler (1707-1783)

- Zrekonstruoval případ $n = 4$ (nekonečný sestup) z Fermatových poznámek.
- Dokázal FLT pro $n = 3$ (1753 zmínka v dopise Goldbachovi, 1770 publikováno). Použil ideu metody nekonečného sestupu, vyžadující ovšem sofistikovanější technické postupy.
- Byl nesvůj z toho, že neví, jak to dokázat obecně. ("*Prohledejte pořádně Fermatovu pozůstalost!*".)

C.F. Gauss (1777-1855)

- Gauss: "*Musím se přiznat, že Fermatova věta jako taková mne zajímá velmi málo; sám mohu uvést mnoho podobných tvrzení, která nelze ani dokázat, ani vyvrátit.*"

1825: Případ $n = 5$ dokázali nezávisle na sobě Dirichlet a Legendre, s využitím metody nekonečného sestupu.

1825: Případ $n = 5$ dokázali nezávisle na sobě Dirichlet a Legendre, s využitím metody nekonečného sestupu.

1836: Případ $n = 7$ dokázal Gabriel Lamé.

1825: Případ $n = 5$ dokázali nezávisle na sobě Dirichlet a Legendre, s využitím metody nekonečného sestupu.

1836: Případ $n = 7$ dokázal Gabriel Lamé.

1847: A. L. Cauchy a G. Lamé víceméně současně tvrdí, že mají obecný důkaz.

1825: Případ $n = 5$ dokázali nezávisle na sobě Dirichlet a Legendre, s využitím metody nekonečného sestupu.

1836: Případ $n = 7$ dokázal Gabriel Lamé.

1847: A. L. Cauchy a G. Lamé víceméně současně tvrdí, že mají obecný důkaz. Na chybu v úvaze v obou těchto důkazech upozornil Joseph Liouville - byla důsledkem výsledků Ernsta Kummera.

Ernst Kummer (1810 – 1893) a nejednoznačnost prvočíselné faktorizace

V množinách např. typu $\mathbb{Z}[\sqrt{-p}]$, (p prvočíslo), neplatí jednoznačnost prvočíselné faktorizace (při jakkoli rozumné definici komplexních prvočísel).

Ernst Kummer (1810 – 1893) a nejednoznačnost prvočíselné faktorizace

V množinách např. typu $\mathbb{Z}[\sqrt{-p}]$, (p prvočíslo), neplatí jednoznačnost prvočíselné faktorizace (při jakkoli rozumné definici komplexních prvočísel). Například v $\mathbb{Z}[\sqrt{-11}] := \{a + bi\sqrt{11},\ a, b \in \mathbb{Z}\}$ je

Ernst Kummer (1810 – 1893) a nejednoznačnost prvočíselné faktorizace

V množinách např. typu $\mathbb{Z}[\sqrt{-p}]$, (p prvočíslo), neplatí jednoznačnost prvočíselné faktorizace (při jakkoli rozumné definici komplexních prvočísel). Například v $\mathbb{Z}[\sqrt{-11}] := \{a + bi\sqrt{11},\ a, b \in \mathbb{Z}\}$ je

$$12 = 2^2 \cdot 3$$

Ernst Kummer (1810 – 1893) a nejednoznačnost prvočíselné faktorizace

V množinách např. typu $\mathbb{Z}[\sqrt{-p}]$, (p prvočíslo), neplatí jednoznačnost prvočíselné faktorizace (při jakkoli rozumné definici komplexních prvočísel). Například v $\mathbb{Z}[\sqrt{-11}] := \{a + bi\sqrt{11},\ a, b \in \mathbb{Z}\}$ je

$$12 = 2^2 \cdot 3 = (1 + i\sqrt{11})(1 - i\sqrt{11})\,.$$

Ernst Kummer (1810 – 1893) a nejednoznačnost prvočíselné faktorizace

V množinách např. typu $\mathbb{Z}[\sqrt{-p}]$, (p prvočíslo), neplatí jednoznačnost prvočíselné faktorizace (při jakkoli rozumné definici komplexních prvočísel). Například v $\mathbb{Z}[\sqrt{-11}] := \{a + bi\sqrt{11},\ a, b \in \mathbb{Z}\}$ je

$$12 = 2^2 \cdot 3 = (1 + i\sqrt{11})(1 - i\sqrt{11})\,.$$

- Kummer: pro některá (tv. regulární) prvočísla p lze tuto chybu obejít. Pro ně FLT dokázal.

Ernst Kummer (1810 – 1893) a nejednoznačnost prvočíselné faktorizace

V množinách např. typu $\mathbb{Z}[\sqrt{-p}]$, (p prvočíslo), neplatí jednoznačnost prvočíselné faktorizace (při jakkoli rozumné definici komplexních prvočísel). Například v $\mathbb{Z}[\sqrt{-11}] := \{a + bi\sqrt{11},\ a, b \in \mathbb{Z}\}$ je

$$12 = 2^2 \cdot 3 = (1 + i\sqrt{11})(1 - i\sqrt{11})\,.$$

- Kummer: pro některá (tv. regulární) prvočísla p lze tuto chybu obejít. Pro ně FLT dokázal. Mezi 3 a 100 včetně jsou jen tři neregulární prvočísla: $37, 59, 67$.

Ernst Kummer (1810 – 1893) a nejednoznačnost prvočíselné faktorizace

V množinách např. typu $\mathbb{Z}[\sqrt{-p}]$, (p prvočíslo), neplatí jednoznačnost prvočíselné faktorizace (při jakkoli rozumné definici komplexních prvočísel). Například v $\mathbb{Z}[\sqrt{-11}] := \{a + bi\sqrt{11},\ a, b \in \mathbb{Z}\}$ je

$$12 = 2^2 \cdot 3 = (1 + i\sqrt{11})(1 - i\sqrt{11})\,.$$

- Kummer: pro některá (tv. regulární) prvočísla p lze tuto chybu obejít. Pro ně FLT dokázal. Mezi 3 a 100 včetně jsou jen tři neregulární prvočísla: $37, 59, 67$. Kummer byl první, kdo dokázal FLT pro takto širokou množinu prvočísel.

Ernst Kummer (1810 – 1893) a nejednoznačnost prvočíselné faktorizace

V množinách např. typu $\mathbb{Z}[\sqrt{-p}]$, (p prvočíslo), neplatí jednoznačnost prvočíselné faktorizace (při jakkoli rozumné definici komplexních prvočísel). Například v $\mathbb{Z}[\sqrt{-11}] := \{a + bi\sqrt{11},\ a, b \in \mathbb{Z}\}$ je

$$12 = 2^2 \cdot 3 = (1 + i\sqrt{11})(1 - i\sqrt{11})\,.$$

- Kummer: pro některá (tv. regulární) prvočísla p lze tuto chybu obejít. Pro ně FLT dokázal. Mezi 3 a 100 včetně jsou jen tři neregulární prvočísla: $37, 59, 67$. Kummer byl první, kdo dokázal FLT pro takto širokou množinu prvočísel.
- Existuje nekonečně mnoho regulárních prvočísel?

Ernst Kummer (1810 – 1893) a nejednoznačnost prvočíselné faktorizace

V množinách např. typu $\mathbb{Z}[\sqrt{-p}]$, (p prvočíslo), neplatí jednoznačnost prvočíselné faktorizace (při jakkoli rozumné definici komplexních prvočísel). Například v $\mathbb{Z}[\sqrt{-11}] := \{a + bi\sqrt{11},\ a, b \in \mathbb{Z}\}$ je

$$12 = 2^2 \cdot 3 = (1 + i\sqrt{11})(1 - i\sqrt{11})\,.$$

- Kummer: pro některá (tv. regulární) prvočísla p lze tuto chybu obejít. Pro ně FLT dokázal. Mezi 3 a 100 včetně jsou jen tři neregulární prvočísla: $37, 59, 67$. Kummer byl první, kdo dokázal FLT pro takto širokou množinu prvočísel.
- Existuje nekonečně mnoho regulárních prvočísel? Dodnes nevíme.

Ernst Kummer (1810 – 1893) a nejednoznačnost prvočíselné faktorizace

V množinách např. typu $\mathbb{Z}[\sqrt{-p}]$, (p prvočíslo), neplatí jednoznačnost prvočíselné faktorizace (při jakkoli rozumné definici komplexních prvočísel). Například v $\mathbb{Z}[\sqrt{-11}] := \{a + bi\sqrt{11},\ a, b \in \mathbb{Z}\}$ je

$$12 = 2^2 \cdot 3 = (1 + i\sqrt{11})(1 - i\sqrt{11})\,.$$

- Kummer: pro některá (tv. regulární) prvočísla p lze tuto chybu obejít. Pro ně FLT dokázal. Mezi 3 a 100 včetně jsou jen tři neregulární prvočísla: $37, 59, 67$. Kummer byl první, kdo dokázal FLT pro takto širokou množinu prvočísel.
- Existuje nekonečně mnoho regulárních prvočísel? Dodnes nevíme. **Bohužel ale existuje nekonečně mnoho neregulárních prvočísel** (1915).

Honorary mention: zamilovaný lékař **Paul Wolfskehl** a jeho odložená sebevražda z r. 1908.

Honorary mention: zamilovaný lékař **Paul Wolfskehl** a jeho odložená sebevražda z r. 1908. Vypsání ceny 100 000 tehdejších německých marek způsobilo nástup armády amatérských řešitelů - fermatistů.

Honorary mention: zamilovaný lékař **Paul Wolfskehl** a jeho odložená sebevražda z r. 1908. Vypsání ceny 100 000 tehdejších německých marek způsobilo nástup armády amatérských řešitelů - fermatistů.

Pozn.: Wolfskehlovu cenu inkasoval Andrew Wiles v červnu 1997, tehdy měla hodnotu 50 tis. USD.

Honorary mention: zamilovaný lékař **Paul Wolfskehl** a jeho odložená sebevražda z r. 1908. Vypsání ceny 100 000 tehdejších německých marek způsobilo nástup armády amatérských řešitelů - fermatistů.

Pozn.: Wolfskehlovu cenu inkasoval Andrew Wiles v červnu 1997, tehdy měla hodnotu 50 tis. USD.

Žádný další významný průlom v klasickém přístupu k FLT se dlouho neodehrál, snad až na rok 1983, kdy Gerd Faltings dokázal tzv. Mordellovu domněnku (z r. 1922),

Honorary mention: zamilovaný lékař **Paul Wolfskehl** a jeho odložená sebevražda z r. 1908. Vypsání ceny 100 000 tehdejších německých marek způsobilo nástup armády amatérských řešitelů - fermatistů.

Pozn.: Wolfskehlovu cenu inkasoval Andrew Wiles v červnu 1997, tehdy měla hodnotu 50 tis. USD.

Žádný další významný průlom v klasickém přístupu k FLT se dlouho neodehrál, snad až na rok 1983, kdy Gerd Faltings dokázal tzv. Mordellovu domněnku (z r. 1922), a sice, že pro každé $n > 2$ má rovnice $x^n + y^n = z^n$ nejvýše konečně mnoho **primitivních** řešení.

Honorary mention: zamilovaný lékař **Paul Wolfskehl** a jeho odložená sebevražda z r. 1908. Vypsání ceny 100 000 tehdejších německých marek způsobilo nástup armády amatérských řešitelů - fermatistů.

Pozn.: Wolfskehlovu cenu inkasoval Andrew Wiles v červnu 1997, tehdy měla hodnotu 50 tis. USD.

Žádný další významný průlom v klasickém přístupu k FLT se dlouho neodehrál, snad až na rok 1983, kdy Gerd Faltings dokázal tzv. Mordellovu domněnku (z r. 1922), a sice, že pro každé $n > 2$ má rovnice $x^n + y^n = z^n$ nejvýše konečně mnoho **primitivních** řešení.

Přesto se hned po 2. světové válce začala rodit teorie, která FLT nakonec zdolala...

4.1. Eliptické křivky

■ 4.1. Eliptické křivky

nejsou elipsy.

■ 4.1. Eliptické křivky

nejsou elipsy. Jde o křivky popsané rovnicí typu

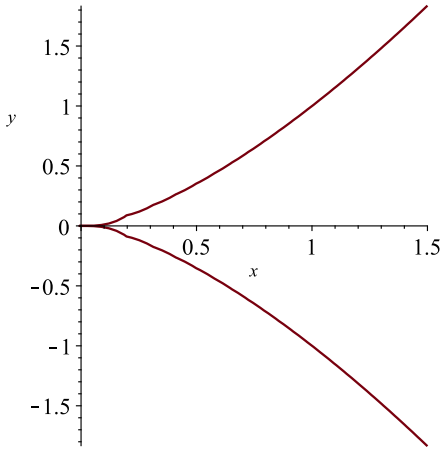
$$y^2 = x^3 + ax^2 + bx + c\,, \quad \text{kde} \quad a, b, c \in \mathbb{Z}\,.$$

■ 4.1. Eliptické křivky

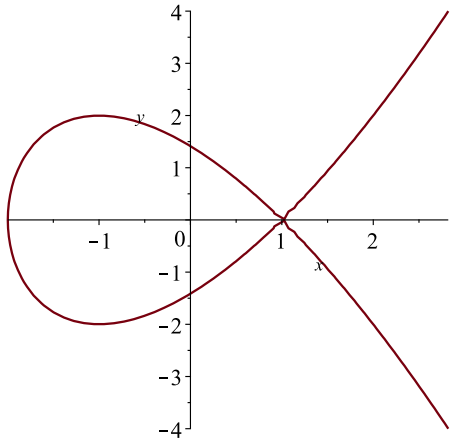
nejsou elipsy. Jde o křivky popsané rovnicí typu

$$y^2 = x^3 + ax^2 + bx + c\,, \quad \text{kde} \quad a, b, c \in \mathbb{Z}\,.$$

Dva jednoduché příklady:

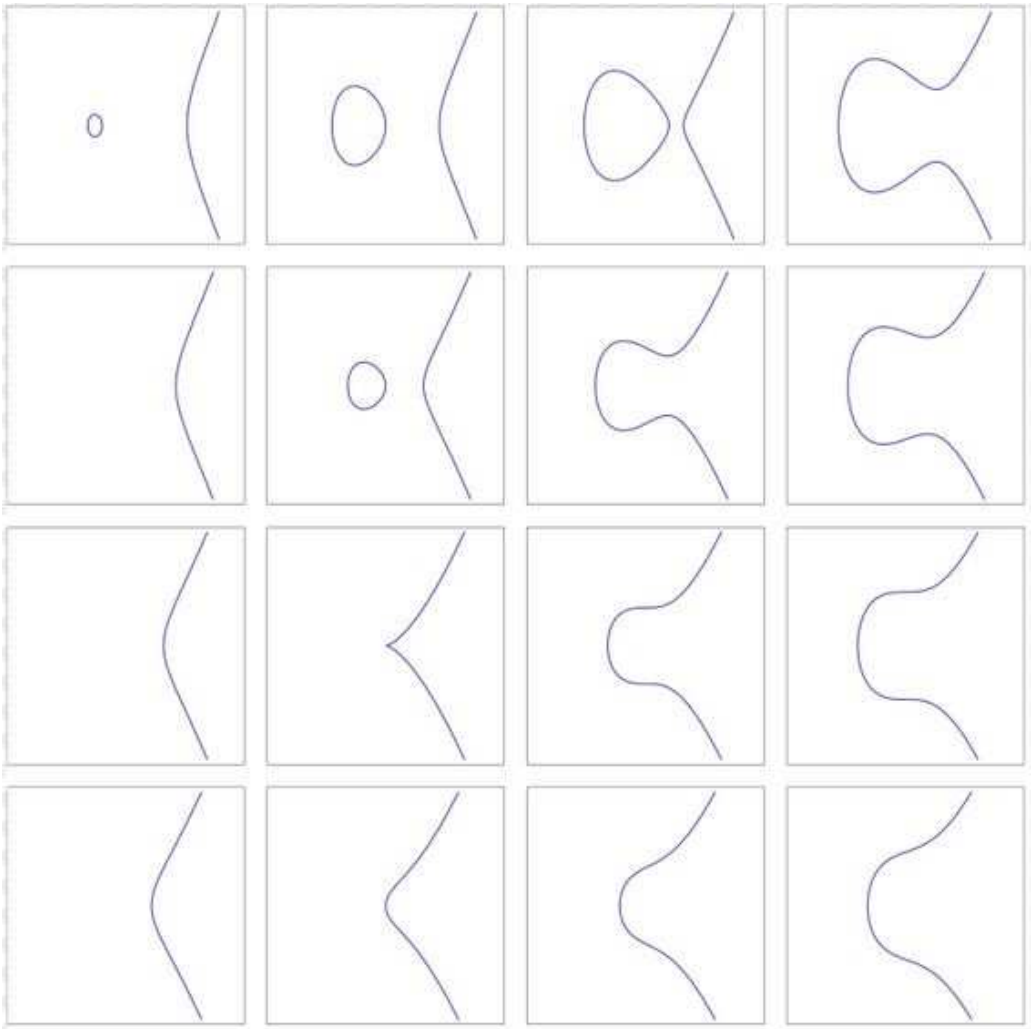


$y^2 = x^3$



$y^2 = x^3 - 3x + 2$

Další typické eliptické křivky



Dnešní využití eliptických křivek - kryptografie.

Dnešní využití eliptických křivek - kryptografie. Znali je už staří Řekové: kolik **celočíselných** (případně racionálních) řešení $[x, y]$ daná rovnice má.

Dnešní využití eliptických křivek - kryptografie. Znali je už staří Řekové: kolik **celočíselných** (případně racionálních) řešení $[x, y]$ daná rovnice má.

Příklad: $y^2 = x^3 - 2$,

Dnešní využití eliptických křivek - kryptografie. Znali je už staří Řekové: kolik **celočíselných** (případně racionálních) řešení $[x, y]$ daná rovnice má.

Příklad: $y^2 = x^3 - 2$, neboli $x^3 - y^2 = 2$,

Dnešní využití eliptických křivek - kryptografie. Znali je už staří Řekové: kolik **celočíselných** (případně racionálních) řešení $[x, y]$ daná rovnice má.

Příklad: $y^2 = x^3 - 2$, neboli $x^3 - y^2 = 2$, neboli jde o nalezení druhé a třetí mocniny, které jsou od sebe vzdálené o hodnotu 2,

Dnešní využití eliptických křivek - kryptografie. Znali je už staří Řekové: kolik **celočíselných** (případně racionálních) řešení $[x, y]$ daná rovnice má.

Příklad: $y^2 = x^3 - 2$, neboli $x^3 - y^2 = 2$, neboli jde o nalezení druhé a třetí mocniny, které jsou od sebe vzdálené o hodnotu 2, neboli hledá se číslo, sevřené mezi druhou a třetí mocninou.

Dnešní využití eliptických křivek - kryptografie. Znali je už staří Řekové: kolik **celočíselných** (případně racionálních) řešení $[x, y]$ daná rovnice má.

Příklad: $y^2 = x^3 - 2$, neboli $x^3 - y^2 = 2$, neboli jde o nalezení druhé a třetí mocniny, které jsou od sebe vzdálené o hodnotu 2, neboli hledá se číslo, sevřené mezi druhou a třetí mocninou.

Fermat: jediné řešení je $[x, y] = [3, 5]$.

Dnešní využití eliptických křivek - kryptografie. Znali je už staří Řekové: kolik **celočíselných** (případně racionálních) řešení $[x, y]$ daná rovnice má.

Příklad: $y^2 = x^3 - 2$, neboli $x^3 - y^2 = 2$, neboli jde o nalezení druhé a třetí mocniny, které jsou od sebe vzdálené o hodnotu 2, neboli hledá se číslo, sevřené mezi druhou a třetí mocninou.

Fermat: jediné řešení je $[x, y] = [3, 5]$.

Pozn: Studují se různé **třídy** (zobecněných) eliptických křivek, například tvaru $y^2 + \alpha y + \beta = x^3 + ax^2 + bx + c$, koeficienty mohou být celočíselné, racionální...

Dnešní využití eliptických křivek - kryptografie. Znali je už staří Řekové: kolik **celočíselných** (případně racionálních) řešení $[x, y]$ daná rovnice má.

Příklad: $y^2 = x^3 - 2$, neboli $x^3 - y^2 = 2$, neboli jde o nalezení druhé a třetí mocniny, které jsou od sebe vzdálené o hodnotu 2, neboli hledá se číslo, sevřené mezi druhou a třetí mocninou.

Fermat: jediné řešení je $[x, y] = [3, 5]$.

Pozn: Studují se různé **třídy** (zobecněných) eliptických křivek, například tvaru $y^2 + \alpha y + \beta = x^3 + ax^2 + bx + c$, koeficienty mohou být celočíselné, racionální...

Křivky tvaru $y^2 = x^3 + ax + b$: neprotínají se a nemají "hroty", pokud $4a^3 + 27b^2 \neq 0$.

Příklad: $y^2 + y = x^3 - x$,

Příklad: $y^2 + y = x^3 - x$, neboli $y(y+1) = x(x^2-1)$.

Příklad: $y^2 + y = x^3 - x$, neboli $y(y+1) = x(x^2-1)$.
Celočíselná řešení?

Příklad: $y^2 + y = x^3 - x$, neboli $y(y+1) = x(x^2-1)$.
Celočíselná řešení? Evidentní řešení:
$[x, y] \in \{[0,0], [0,-1], [1,0], [1,-1], [-1,0], [-1,-1]\}$.

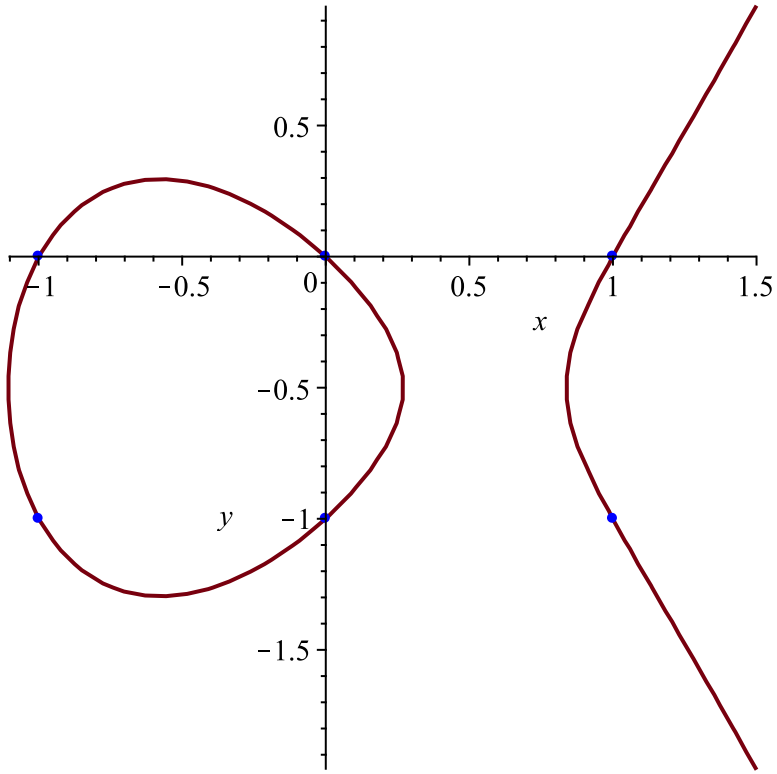
Příklad: $y^2 + y = x^3 - x$, neboli $y(y+1) = x(x^2-1)$.
Celočíselná řešení? Evidentní řešení:
$[x, y] \in \{[0,0], [0,-1], [1,0], [1,-1], [-1,0], [-1,-1]\}$. A dál?

Příklad: $y^2 + y = x^3 - x$, neboli $y(y+1) = x(x^2-1)$.
Celočíselná řešení? Evidentní řešení:
$[x, y] \in \{[0,0], [0,-1], [1,0], [1,-1], [-1,0], [-1,-1]\}$. A dál?

Obecně je velmi těžké najít všechna řešení (mezi **nekonečné mnoha** možnými kandidáty na řešení.)

Příklad: $y^2 + y = x^3 - x$, neboli $y(y+1) = x(x^2-1)$.
Celočíselná řešení? Evidentní řešení:
$[x, y] \in \{[0,0], [0,-1], [1,0], [1,-1], [-1,0], [-1,-1]\}$. A dál?

Obecně je velmi těžké najít všechna řešení (mezi **nekonečné mnoha** možnými kandidáty na řešení.)



Proto vznikla myšlenka hledat řešení **v konečných (modulárních) aritmetikách**.

Proto vznikla myšlenka hledat řešení **v konečných (modulárních) aritmetikách**.

Studujeme naši rovnici $y^2 + y = x^3 - x$,

Proto vznikla myšlenka hledat řešení **v konečných (modulárních) aritmetikách**.

Studujeme naši rovnici $y^2 + y = x^3 - x$, neboli $y(y+1) = x(x^2-1)$

Proto vznikla myšlenka hledat řešení **v konečných (modulárních) aritmetikách**.

Studujeme naši rovnici $y^2 + y = x^3 - x$, neboli $y(y+1) = x(x^2-1)$ v různých modulárních aritmetikách (tj. jen s konečným počtem kandidátů na řešení).

Proto vznikla myšlenka hledat řešení **v konečných (modulárních) aritmetikách**.

Studujeme naši rovnici $y^2 + y = x^3 - x$, neboli $y(y+1) = x(x^2-1)$ v různých modulárních aritmetikách (tj. jen s konečným počtem kandidátů na řešení).

Například v aritmetice mod 3 stačí zvažovat $x \in \{0, 1, 2\}$, $y \in \{0, 1, 2\}$ a počítat modulo 3:

Proto vznikla myšlenka hledat řešení **v konečných (modulárních) aritmetikách**.

Studujeme naši rovnici $y^2 + y = x^3 - x$, neboli $y(y+1) = x(x^2-1)$ v různých modulárních aritmetikách (tj. jen s konečným počtem kandidátů na řešení).

Například v aritmetice mod 3 stačí zvažovat $x \in \{0, 1, 2\}$, $y \in \{0, 1, 2\}$ a počítat modulo 3: třeba pro $y = 2$ je

Proto vznikla myšlenka hledat řešení **v konečných (modulárních) aritmetikách**.

Studujeme naši rovnici $y^2 + y = x^3 - x$, neboli $y(y+1) = x(x^2-1)$ v různých modulárních aritmetikách (tj. jen s konečným počtem kandidátů na řešení).

Například v aritmetice mod 3 stačí zvažovat $x \in \{0,1,2\}$, $y \in \{0,1,2\}$ a počítat modulo 3: třeba pro $y = 2$ je

$$\text{LHS} = 2^2 + 2 = 6$$

Proto vznikla myšlenka hledat řešení **v konečných (modulárních) aritmetikách**.

Studujeme naši rovnici $y^2 + y = x^3 - x$, neboli $y(y+1) = x(x^2-1)$ v různých modulárních aritmetikách (tj. jen s konečným počtem kandidátů na řešení).

Například v aritmetice mod 3 stačí zvažovat $x \in \{0,1,2\}$, $y \in \{0,1,2\}$ a počítat modulo 3: třeba pro $y = 2$ je

$$\text{LHS} = 2^2 + 2 = 6 \equiv 0 \pmod 3.$$

Proto vznikla myšlenka hledat řešení **v konečných (modulárních) aritmetikách**.

Studujeme naši rovnici $y^2 + y = x^3 - x$, neboli $y(y+1) = x(x^2-1)$ v různých modulárních aritmetikách (tj. jen s konečným počtem kandidátů na řešení).

Například v aritmetice mod 3 stačí zvažovat $x \in \{0,1,2\}$, $y \in \{0,1,2\}$ a počítat modulo 3: třeba pro $y = 2$ je

$$\text{LHS} = 2^2 + 2 = 6 \equiv 0 \pmod 3.$$

Jednoduše zjistíme, že v aritmetice mod 3 má rovnice právě 6 řešení:

$$[x,y] \in \{[0,0],[0,2],[1,0],[1,2],[2,0],[2,2]\},$$

Proto vznikla myšlenka hledat řešení **v konečných (modulárních) aritmetikách**.

Studujeme naši rovnici $y^2 + y = x^3 - x$, neboli $y(y+1) = x(x^2-1)$ v různých modulárních aritmetikách (tj. jen s konečným počtem kandidátů na řešení).

Například v aritmetice mod 3 stačí zvažovat $x \in \{0,1,2\}$, $y \in \{0,1,2\}$ a počítat modulo 3: třeba pro $y = 2$ je

$$\text{LHS} = 2^2 + 2 = 6 \equiv 0 \pmod 3.$$

Jednoduše zjistíme, že v aritmetice mod 3 má rovnice právě 6 řešení:

$$[x,y] \in \{[0,0],[0,2],[1,0],[1,2],[2,0],[2,2]\},$$

což zapíšeme $E_3 = 6$.

Pro námi zvažovanou křivku lze ukázat

Pro námi zvažovanou křivku lze ukázat

$$E_1 = 1, E_2 = 4, \quad E_3 = 6, \quad E_4 = 8, \quad E_5 = 7, \quad \ldots,$$

Pro námi zvažovanou křivku lze ukázat

$$E_1 = 1, E_2 = 4, \quad E_3 = 6, \quad E_4 = 8, \quad E_5 = 7, \quad \ldots,$$

jinak zapsáno, pro E_2 až E_{11},

$$E = [1, 4, 6, 8, 7, 24, 8, 16, 18, 28, 16 \ldots].$$

Pro námi zvažovanou křivku lze ukázat

$$E_1 = 1, E_2 = 4, \quad E_3 = 6, \quad E_4 = 8, \quad E_5 = 7, \quad \ldots,$$

jinak zapsáno, pro E_2 až E_{11},

$$E = [1, 4, 6, 8, 7, 24, 8, 16, 18, 28, 16 \ldots].$$

Jde o tzv. **E-řadu křivky** $y^2 + y = x^3 - x$.

Pro námi zvažovanou křivku lze ukázat

$$E_1 = 1, E_2 = 4, \quad E_3 = 6, \quad E_4 = 8, \quad E_5 = 7, \quad \ldots,$$

jinak zapsáno, pro E_2 až E_{11},

$$E = [1, 4, 6, 8, 7, 24, 8, 16, 18, 28, 16 \ldots].$$

Jde o tzv. **E-řadu křivky** $y^2 + y = x^3 - x$. Ukazuje se, že **v jisté dobře definované třídě eliptických křivek charakterizují prvočíselné členy E-řady danou křivku jednoznačně.**

Pro námi zvažovanou křivku lze ukázat

$$E_1 = 1, E_2 = 4, \quad E_3 = 6, \quad E_4 = 8, \quad E_5 = 7, \quad \ldots,$$

jinak zapsáno, pro E_2 až E_{11},

$$E = [1, 4, 6, 8, 7, 24, 8, 16, 18, 28, 16 \ldots].$$

Jde o tzv. **E-řadu křivky** $y^2 + y = x^3 - x$. Ukazuje se, že **v jisté dobře definované třídě eliptických křivek charakterizují prvočíselné členy E-řady danou křivku jednoznačně.** Je to jakýsi její "DNA-kód", pomocí kterého lze křivku jednoznačně určit.

$$E = [1, 4, 6, 8, 7, 24, 8, 16, 18, 28, 16 \ldots].$$

4.2. Modulární formy

4.2. Modulární formy

jsou velmi složité matematické objekty, která si zaslouží nejprve přesnou definici a až poté i jakési vysvětlení.

4.2. Modulární formy

jsou velmi složité matematické objekty, která si zaslouží nejprve přesnou definici a až poté i jakési vysvětlení.

Definice

Modulární formou s vahou $k \in \mathbb{N}$

4.2. Modulární formy

jsou velmi složité matematické objekty, která si zaslouží nejprve přesnou definici a až poté i jakési vysvětlení.

Definice

Modulární formou s vahou $k \in \mathbb{N}$ nazvu komplexní funkci komplexní proměnné f,

4.2. Modulární formy

jsou velmi složité matematické objekty, která si zaslouží nejprve přesnou definici a až poté i jakési vysvětlení.

Definice

Modulární formou s vahou $k \in \mathbb{N}$ nazvu komplexní funkci komplexní proměnné f, která je definována a je holomorfní na horní komplexní polorovině $H := \{z \in \mathbb{C};\ \mathrm{Im}(z) > 0\}$,

4.2. Modulární formy

jsou velmi složité matematické objekty, která si zaslouží nejprve přesnou definici a až poté i jakési vysvětlení.

Definice

Modulární formou s vahou $k \in \mathbb{N}$ nazvu komplexní funkci komplexní proměnné f, která je definována a je holomorfní na horní komplexní polorovině $H := \{z \in \mathbb{C};\ \mathrm{Im}(z) > 0\}$, a která navíc splňuje

4.2. Modulární formy

jsou velmi složité matematické objekty, která si zaslouží nejprve přesnou definici a až poté i jakési vysvětlení.

Definice

Modulární formou s vahou $k \in \mathbb{N}$ nazvu komplexní funkci komplexní proměnné f, která je definována a je holomorfní na horní komplexní polorovině $H := \{z \in \mathbb{C};\ \mathrm{Im}(z) > 0\}$, a která navíc splňuje

- $f(iz)$ je omezená pro $z \to \infty$;

4.2. Modulární formy

jsou velmi složité matematické objekty, která si zaslouží nejprve přesnou definici a až poté i jakési vysvětlení.

Definice

Modulární formou s vahou $k \in \mathbb{N}$ nazvu komplexní funkci komplexní proměnné f, která je definována a je holomorfní na horní komplexní polorovině $H := \{z \in \mathbb{C};\ \mathrm{Im}(z) > 0\}$, a která navíc splňuje

- $f(iz)$ je omezená pro $z \to \infty$;
- $f(\frac{az+b}{cz+d}) = (cz + d)^k f(z)$ pro všechna $z \in H$

4.2. Modulární formy

jsou velmi složité matematické objekty, která si zaslouží nejprve přesnou definici a až poté i jakési vysvětlení.

Definice

Modulární formou s vahou $k \in \mathbb{N}$ nazvu komplexní funkci komplexní proměnné f, která je definována a je holomorfní na horní komplexní polorovině $H := \{z \in \mathbb{C};\ \mathrm{Im}(z) > 0\}$, a která navíc splňuje

- $f(iz)$ je omezená pro $z \to \infty$;
- $f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$ pro všechna $z \in H$ a pro všechna $a, b, c, d \in \mathbb{Z}$ taková, že $ad - bc = 1$.

4.2. Modulární formy

jsou velmi složité matematické objekty, která si zaslouží nejprve přesnou definici a až poté i jakési vysvětlení.

Definice

Modulární formou s vahou $k \in \mathbb{N}$ nazvu komplexní funkci komplexní proměnné f, která je definována a je holomorfní na horní komplexní polorovině $H := \{z \in \mathbb{C};\ \mathrm{Im}(z) > 0\}$, a která navíc splňuje

- $f(iz)$ je omezená pro $z \to \infty$;
- $f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$ pro všechna $z \in H$ a pro všechna $a, b, c, d \in \mathbb{Z}$ taková, že $ad - bc = 1$.

Druhá podmínka je velmi silná – na funkci f klademe nekonečně mnoho podmínek typu "symetrie".

$f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$ pro všechna $z \in H$ a pro všechna $a, b, c, d \in \mathbb{Z}$ taková, že $ad - bc = 1$.

$f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$ pro všechna $z \in H$ a pro všechna $a, b, c, d \in \mathbb{Z}$ taková, že $ad - bc = 1$.

To tedy znamená, že všechny následující vztahy musí platit pro všechna $z \in H$:

$f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$ pro všechna $z \in H$ a pro všechna $a, b, c, d \in \mathbb{Z}$ taková, že $ad - bc = 1$.

To tedy znamená, že všechny následující vztahy musí platit pro všechna $z \in H$:

- a=1, c=0, b=1, d=1: $f(z+1) = f(z)$,

$f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$ pro všechna $z \in H$ a pro všechna $a, b, c, d \in \mathbb{Z}$ taková, že $ad - bc = 1$.

To tedy znamená, že všechny následující vztahy musí platit pro všechna $z \in H$:

- a=1, c=0, b=1, d=1: $f(z+1) = f(z)$,
- a=0, b=−1, c=1, d=0: $f(-\frac{1}{z}) = z^k f(z)$,
- ...

$f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$ pro všechna $z \in H$ a pro všechna $a, b, c, d \in \mathbb{Z}$ taková, že $ad - bc = 1$.

To tedy znamená, že všechny následující vztahy musí platit pro všechna $z \in H$:

- a=1, c=0, b=1, d=1: $f(z+1) = f(z)$,
- a=0, b=−1, c=1, d=0: $f(-\frac{1}{z}) = z^k f(z)$,
- ...
- a=3, b=7, c= 2, d=5: $f(\frac{3z+7}{2z+5}) = (2z+5)^k f(z)$,

$f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$ pro všechna $z \in H$ a pro všechna $a, b, c, d \in \mathbb{Z}$ taková, že $ad - bc = 1$.

To tedy znamená, že všechny následující vztahy musí platit pro všechna $z \in H$:

- a=1, c=0, b=1, d=1: $f(z+1) = f(z)$,
- a=0, b=−1, c=1, d=0: $f(-\frac{1}{z}) = z^k f(z)$,
- ...
- a=3, b=7, c= 2, d=5: $f(\frac{3z+7}{2z+5}) = (2z+5)^k f(z)$,
- ...

Dlouho nebylo jasné, jestli funkce, splňující tolik podmínek, vůbec existují...

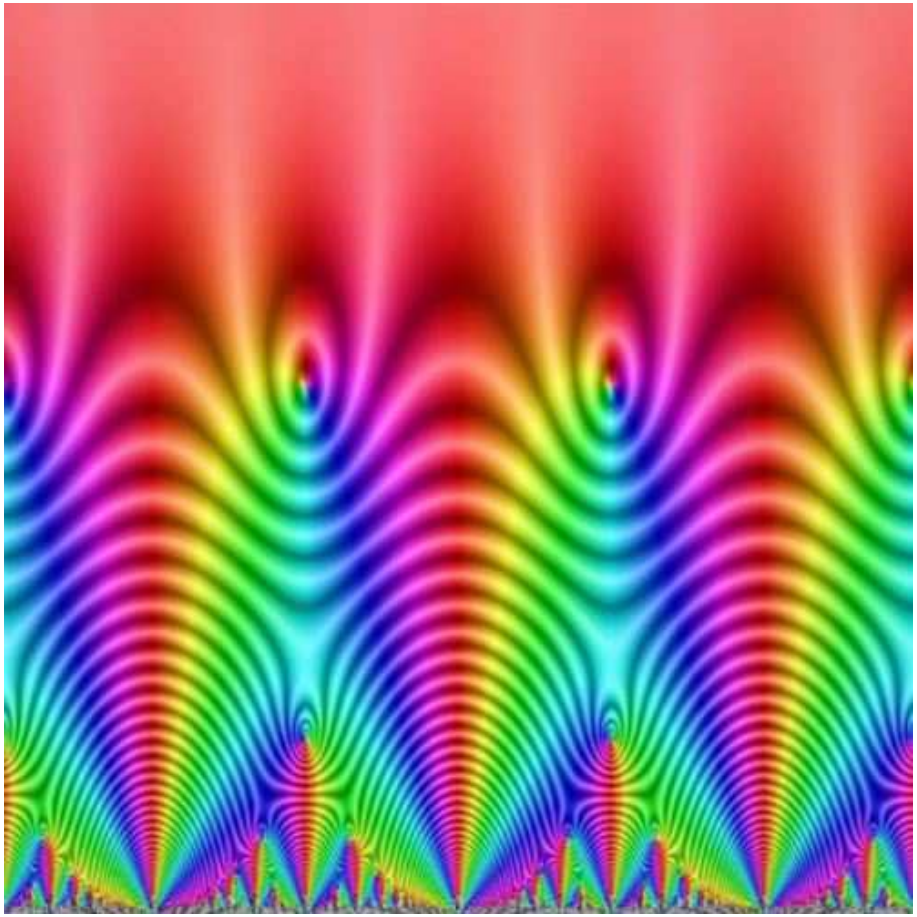
$f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$ pro všechna $z \in H$ a pro všechna $a, b, c, d \in \mathbb{Z}$ taková, že $ad - bc = 1$.

To tedy znamená, že všechny následující vztahy musí platit pro všechna $z \in H$:

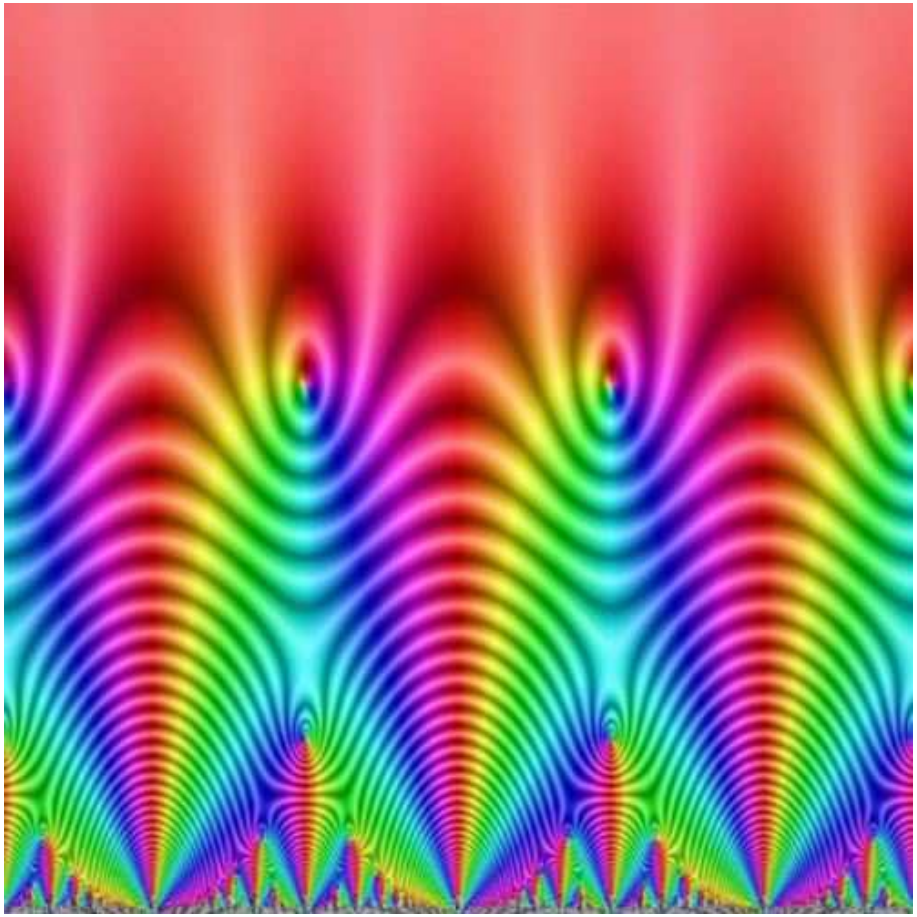
- a=1, c=0, b=1, d=1: $f(z+1) = f(z)$,
- a=0, b=−1, c=1, d=0: $f(-\frac{1}{z}) = z^k f(z)$,
- ...
- a=3, b=7, c= 2, d=5: $f(\frac{3z+7}{2z+5}) = (2z+5)^k f(z)$,
- ...

Dlouho nebylo jasné, jestli funkce, splňující tolik podmínek, vůbec existují...

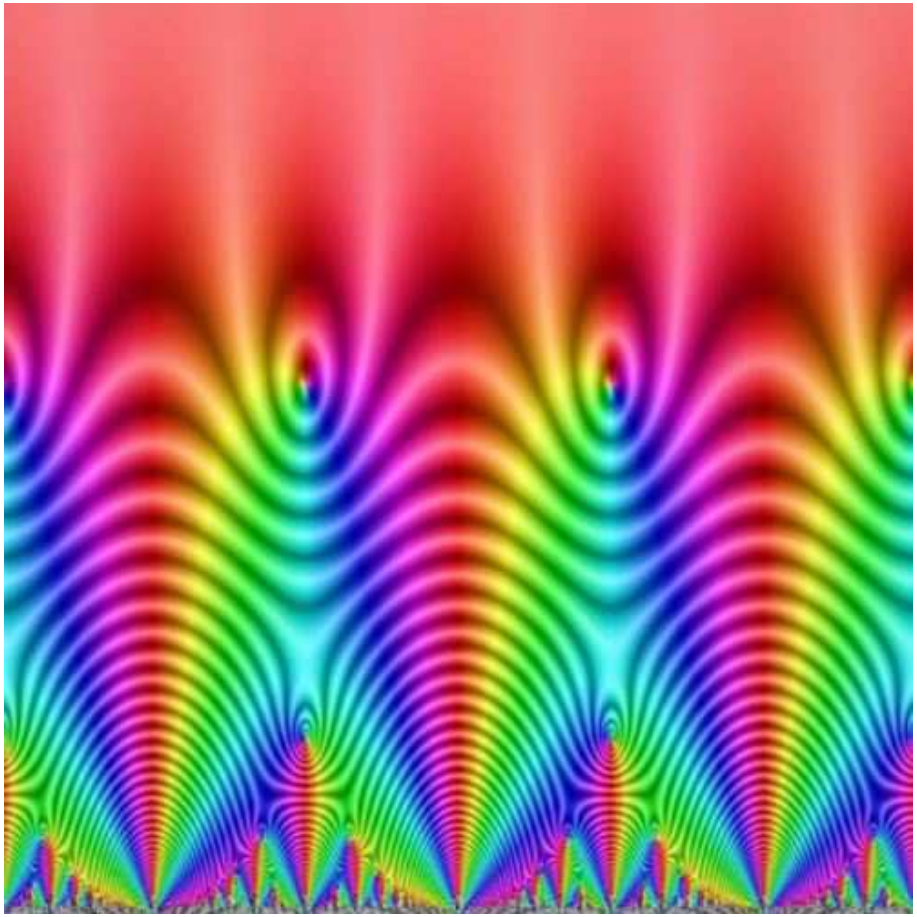
Totiž: k liché $\Longrightarrow$ podmínky splňuje jedině $f \equiv 0$



- Definiční obor modulární formy: body stejné barvy musí mít stejnou hodnotu.



- Definiční obor modulární formy: body stejné barvy musí mít stejnou hodnotu.
- Symetrie: posun, reflexe, fraktální symetrie.



- Definiční obor modulární formy: body stejné barvy musí mít stejnou hodnotu.
- Symetrie: posun, reflexe, fraktální symetrie.
- Přesto: existuje nekonečně mnoho modulárních forem (např.) s vahou $k=2$.

Zopakujme:

$$f(z+1) = f(z)$$

Zopakujme:

$$f(z+1) = f(z) \quad \Longrightarrow \quad f(z) = \sum_{n=0}^{\infty} m_n q^n \,,$$

Zopakujme:

$$f(z+1) = f(z) \quad \Longrightarrow \quad f(z) = \sum_{n=0}^{\infty} m_n q^n\,, \quad q = e^{2\pi i n z}\,.$$

Zopakujme:

$$f(z+1) = f(z) \quad \Longrightarrow \quad f(z) = \sum_{n=0}^{\infty} m_n q^n\,, \quad q = e^{2\pi i n z}\,.$$

. . . Fourierova řada.

Zopakujme:

$$f(z+1) = f(z) \quad \Longrightarrow \quad f(z) = \sum_{n=0}^{\infty} m_n q^n\,, \quad q = e^{2\pi i n z}.$$

. . . Fourierova řada.

Modulární formy jsou tedy charakterizované koeficienty své Fourierovy řady, tzv. M-řadou

$$M = [m_0, m_1, m_2, m_3, m_4 \ldots].$$

Zopakujme:

$$f(z+1) = f(z) \quad \Longrightarrow \quad f(z) = \sum_{n=0}^{\infty} m_n q^n\,, \quad q = e^{2\pi i n z}.$$

. . . Fourierova řada.

Modulární formy jsou tedy charakterizované koeficienty své Fourierovy řady, tzv. M-řadou

$$M = [m_0, m_1, m_2, m_3, m_4 \ldots].$$

Například pro modulární formu, charakterizovanou Fourierovou řadou (musí se nicméně ukázat, že splňuje všechny ty symetrie . . .):

Zopakujme:

$$f(z+1) = f(z) \quad \Longrightarrow \quad f(z) = \sum_{n=0}^{\infty} m_n q^n\,, \quad q = e^{2\pi i n z}.$$

. . . Fourierova řada.

Modulární formy jsou tedy charakterizované koeficienty své Fourierovy řady, tzv. M-řadou

$$M = [m_0, m_1, m_2, m_3, m_4 \ldots].$$

Například pro modulární formu, charakterizovanou Fourierovou řadou (musí se nicméně ukázat, že splňuje všechny ty symetrie . . .):

$$f(z) = q - 2q^2 - 3q^3 + 2q^4 - 2q^5 + 6q^6 - q^7 + 6q^9 + 4q^{10} - 5q^{11} \cdots\,,$$

kde $q = e^{2\pi i z}$, získáme M-řadu

$$M = [1, -2, -3, 2, -2, 6, -1, 0, 6, 4, -5 \ldots].$$

Jména k zapamatování: Jutaka Taniyama (1927-1958), Goro Shimura (1930-2019).

Jména k zapamatování: Jutaka Taniyama (1927-1958), Goro Shimura (1930-2019).

Taniyama si všiml, že jisté členy M-řady jím studované modulární formy lze zrekonstuovat pomocí odpovídajících členů E-řady jedné eliptické rovnice.

$$E = [1,\ 4,\ 6, 8,\ 7, 24,\ 8, 16, 18, 28, 16 \ldots].$$
$$M = [1, -2, -3, 2, -2,\ 6, -1,\ 0,\ 6,\ 4, -5 \ldots].$$

Jména k zapamatování: Jutaka Taniyama (1927-1958), Goro Shimura (1930-2019).

Taniyama si všiml, že jisté členy M-řady jím studované modulární formy lze zrekonstuovat pomocí odpovídajících členů E-řady jedné eliptické rovnice.

$$E = [1,\ 4,\ 6, 8,\ 7, 24,\ 8, 16, 18, 28, 16 \ldots].$$
$$M = [1, -2, -3, 2, -2,\ 6, -1,\ 0,\ 6,\ 4, -5 \ldots].$$

$$E = [1,\ 4,\ 6, 8,\ 7, 24,\ 8, 16, 18, 28, 16 \ldots].$$
$$M = [1, -2, -3, 2, -2,\ 6, -1,\ 0,\ 6,\ 4, -5 \ldots].$$

Jména k zapamatování: Jutaka Taniyama (1927-1958), Goro Shimura (1930-2019).

Taniyama si všiml, že jisté členy M-řady jím studované modulární formy lze zrekonstuovat pomocí odpovídajících členů E-řady jedné eliptické rovnice.

$$E = [1,\ 4,\ 6, 8,\ 7, 24,\ 8, 16, 18, 28, 16 \ldots].$$
$$M = [1, -2, -3, 2, -2,\ 6, -1,\ 0,\ 6,\ 4, -5 \ldots].$$

$$E = [1,\ 4,\ 6, 8,\ 7, 24,\ 8, 16, 18, 28, 16 \ldots].$$
$$M = [1, -2, -3, 2, -2,\ 6, -1,\ 0,\ 6,\ 4, -5 \ldots].$$
$$\mathbb{N} = [1, 2, 3, 4, 5,\ 6, 7,\ 8,\ 9,\ 10, 11 \ldots].$$

Jména k zapamatování: Jutaka Taniyama (1927-1958), Goro Shimura (1930-2019).

Taniyama si všiml, že jisté členy M-řady jím studované modulární formy lze zrekonstuovat pomocí odpovídajících členů E-řady jedné eliptické rovnice.

$$E = [1,\ 4,\ 6, 8,\ 7, 24,\ 8, 16, 18, 28, 16 \ldots].$$
$$M = [1, -2, -3, 2, -2,\ 6, -1,\ 0,\ 6,\ 4, -5 \ldots].$$

$$E = [1,\ 4,\ 6, 8,\ 7, 24,\ 8, 16, 18, 28, 16 \ldots].$$
$$M = [1, -2, -3, 2, -2,\ 6, -1,\ 0,\ 6,\ 4, -5 \ldots].$$
$$\mathbb{N} = [1, 2, 3, 4, 5,\ 6, 7,\ 8,\ 9,\ 10, 11 \ldots].$$

$$E_p + m_p = p\,, \qquad \text{pro } p \text{ prvočíslo}\,.$$

4.3. Tušení souvislosti

4.3. Tušení souvislosti

Taniyama spolu s Shimurou vyslovili v r. 1955 smělou hypotézu, dalších 40 let označovanou jako

Taniyamova-Shimurova(-Weilova) hypotéza

(. . . Weilova od 70. let), říkající *v podstatě* toto:

■ 4.3. Tušení souvislosti

Taniyama spolu s Shimurou vyslovili v r. 1955 smělou hypotézu, dalších 40 let označovanou jako

Taniyamova-Shimurova(-Weilova) hypotéza

(. . . Weilova od 70. let), říkající *v podstatě* toto:

> Nechť E je eliptická křivka nad $\mathbb{Q}$ s E-řadou E_n. Potom existuje jednoznačně určená modulární forma s vahou 2, přičemž pro členy m_n její M-řady platí $m_1=1$ a $m_p=p-E_p$, pro všechna prvočísla p.

4.3. Tušení souvislosti

Taniyama spolu s Shimurou vyslovili v r. 1955 smělou hypotézu, dalších 40 let označovanou jako

Taniyamova-Shimurova(-Weilova) hypotéza

(. . . Weilova od 70. let), říkající *v podstatě* toto:

> Nechť E je eliptická křivka nad $\mathbb{Q}$ s E-řadou E_n. Potom existuje jednoznačně určená modulární forma s vahou 2, přičemž pro členy m_n její M-řady platí $m_1=1$ a $m_p=p-E_p$, pro všechna prvočísla p.

Jde o velmi hluboké tvrzení z teorie čísel, které však až do roku cca 1982 nemělo žádnou souvislost s FLT. Až v roce 1982...

5. Průlet kolem Wilesova důkazu

- **5.1. Gerhard Frey (*1944)**

5.1. Gerhard Frey (*1944)

překvapil v r. 1982 všechny číselné teoretiky:

5.1. Gerhard Frey (*1944)

překvapil v r. 1982 všechny číselné teoretiky:

Pokud platí $a^p + b^p = c^p$ pro nějaká přirozená a, b, c a prvočíslo $p > 5$, tak se zdá, že eliptické křivce

$$y^2 = x(x - a^p)(x + b^p)$$

neodpovídá žádná modulární forma (která by ovšem podle T-S-W hypotézy měla existovat).

5.1. Gerhard Frey (*1944)

překvapil v r. 1982 všechny číselné teoretiky:

> Pokud platí $a^p + b^p = c^p$ pro nějaká přirozená a, b, c a prvočíslo $p > 5$, tak se zdá, že eliptické křivce
>
> $$y^2 = x(x - a^p)(x + b^p)$$
>
> neodpovídá žádná modulární forma (která by ovšem podle T-S-W hypotézy měla existovat).

Toto Freyovo "podezření" (zvané ε-hypotéza) v r. 1986 **dokázal** Ken Ribet (*1948).

5.1. Gerhard Frey (*1944)

překvapil v r. 1982 všechny číselné teoretiky:

> Pokud platí $a^p + b^p = c^p$ pro nějaká přirozená a, b, c a prvočíslo $p > 5$, tak se zdá, že eliptické křivce
>
> $$y^2 = x(x - a^p)(x + b^p)$$
>
> neodpovídá žádná modulární forma (která by ovšem podle T-S-W hypotézy měla existovat).

Toto Freyovo "podezření" (zvané ε-hypotéza) v r. 1986 **dokázal** Ken Ribet (*1948). (Od té doby se **ε-hypotéze** říká Ribetova věta).

Od té chvíle bylo jasné, že mohou nastat jen dvě situace:

Od té chvíle bylo jasné, že mohou nastat jen dvě situace:

1. Existuje řešení Fermatovy rovnice $a^p + b^p = c^p$ pro nějaká přirozená a, b, c a prvočíslo $p > 5$.

Od té chvíle bylo jasné, že mohou nastat jen dvě situace:

1. Existuje řešení Fermatovy rovnice $a^p + b^p = c^p$ pro nějaká přirozená a, b, c a prvočíslo $p > 5$. Pak ovšem neplatí T-S-W hypotéza, protože ji vyvrací Freyova křivka $y^2 = x(x - a^p)(x + b^p)$.

Od té chvíle bylo jasné, že mohou nastat jen dvě situace:

1. Existuje řešení Fermatovy rovnice $a^p + b^p = c^p$ pro nějaká přirozená a, b, c a prvočíslo $p > 5$. Pak ovšem neplatí T-S-W hypotéza, protože ji vyvrací Freyova křivka $y^2 = x(x - a^p)(x + b^p)$.
2. Platí T-S-W hypotéza, a tedy žádná "Freyova křivka" nemůže existovat.

Od té chvíle bylo jasné, že mohou nastat jen dvě situace:

1. Existuje řešení Fermatovy rovnice $a^p + b^p = c^p$ pro nějaká přirozená a, b, c a prvočíslo $p > 5$. Pak ovšem neplatí T-S-W hypotéza, protože ji vyvrací Freyova křivka $y^2 = x(x - a^p)(x + b^p)$.
2. Platí T-S-W hypotéza, a tedy žádná "Freyova křivka" nemůže existovat. Pokud ale neexistuje Freyova křivka, tak ani neexistují přirozená a, b, c a prvočíslo $p > 5$ taková, že platí $a^p + b^p = c^p$.

Od té chvíle bylo jasné, že mohou nastat jen dvě situace:

1. Existuje řešení Fermatovy rovnice $a^p + b^p = c^p$ pro nějaká přirozená a, b, c a prvočíslo $p > 5$. Pak ovšem neplatí T-S-W hypotéza, protože ji vyvrací Freyova křivka $y^2 = x(x - a^p)(x + b^p)$.
2. Platí T-S-W hypotéza, a tedy žádná "Freyova křivka" nemůže existovat. Pokud ale neexistuje Freyova křivka, tak ani neexistují přirozená a, b, c a prvočíslo $p > 5$ taková, že platí $a^p + b^p = c^p$. To ale znamená, že platí FLT pro $p > 5$.

Od té chvíle bylo jasné, že mohou nastat jen dvě situace:

1. Existuje řešení Fermatovy rovnice $a^p + b^p = c^p$ pro nějaká přirozená a, b, c a prvočíslo $p > 5$. Pak ovšem neplatí T-S-W hypotéza, protože ji vyvrací Freyova křivka $y^2 = x(x - a^p)(x + b^p)$.
2. Platí T-S-W hypotéza, a tedy žádná "Freyova křivka" nemůže existovat. Pokud ale neexistuje Freyova křivka, tak ani neexistují přirozená a, b, c a prvočíslo $p > 5$ taková, že platí $a^p + b^p = c^p$. To ale znamená, že platí FLT pro $p > 5$.

Stručně řečeno:

Od té chvíle bylo jasné, že mohou nastat jen dvě situace:

1. Existuje řešení Fermatovy rovnice $a^p + b^p = c^p$ pro nějaká přirozená a, b, c a prvočíslo $p > 5$. Pak ovšem neplatí T-S-W hypotéza, protože ji vyvrací Freyova křivka $y^2 = x(x - a^p)(x + b^p)$.
2. Platí T-S-W hypotéza, a tedy žádná "Freyova křivka" nemůže existovat. Pokud ale neexistuje Freyova křivka, tak ani neexistují přirozená a, b, c a prvočíslo $p > 5$ taková, že platí $a^p + b^p = c^p$. To ale znamená, že platí FLT pro $p > 5$.

Stručně řečeno:

T-S-W hypotéza implikuje Velkou Fermatovu větu.

5.2. Andrew Wiles

(*1953, Cambridge)

- V 10 letech objevil v knihovně knihu o FLT a rozhodl se, že bude tím, kdo ji jednou dokáže.

5.2. Andrew Wiles

(*1953, Cambridge)

- V 10 letech objevil v knihovně knihu o FLT a rozhodl se, že bude tím, kdo ji jednou dokáže.
- Bc. v Oxfordu, Ph.D v Cambridge, profesura v Princetonu.

5.2. Andrew Wiles

(*1953, Cambridge)

- V 10 letech objevil v knihovně knihu o FLT a rozhodl se, že bude tím, kdo ji jednou dokáže.
- Bc. v Oxfordu, Ph.D v Cambridge, profesura v Princetonu.
- Od roku 1975 pracoval pod vedením Johna Coatese na teorii eliptických křivek (aniž tušil, že T-S-W hypotéza je klíčem k FLT).

5.2. Andrew Wiles

(*1953, Cambridge)

- V 10 letech objevil v knihovně knihu o FLT a rozhodl se, že bude tím, kdo ji jednou dokáže.
- Bc. v Oxfordu, Ph.D v Cambridge, profesura v Princetonu.
- Od roku 1975 pracoval pod vedením Johna Coatese na teorii eliptických křivek (aniž tušil, že T-S-W hypotéza je klíčem k FLT).
- Poté, co Ken Ribet dokázal v r. 1986 tvrzení o Freyově křivce se Wiles rozhodl pracovat v ústraní na důkazu T-S-W hypotézy.

5.2. Andrew Wiles

(*1953, Cambridge)

- V 10 letech objevil v knihovně knihu o FLT a rozhodl se, že bude tím, kdo ji jednou dokáže.
- Bc. v Oxfordu, Ph.D v Cambridge, profesura v Princetonu.
- Od roku 1975 pracoval pod vedením Johna Coatese na teorii eliptických křivek (aniž tušil, že T-S-W hypotéza je klíčem k FLT).
- Poté, co Ken Ribet dokázal v r. 1986 tvrzení o Freyově křivce se Wiles rozhodl pracovat v ústraní na důkazu T-S-W hypotézy.
- Po 7 letech práce, v červnu 1993, byl přesvědčen, že nalezl důkaz a sezval kolegy na sérii tří přednášek.


To ensure (1) holds we use Hilbert irreducibility
Pick a
Then pick a
5-adic rep^n on E is

23.6.1993: "I think I'll stop here. . ."

5.3. Poslední překážka

5.3. Poslední překážka

- Důkaz měl více než stovku stran a byl podroben přísnému zkoumání největších expertů v oboru.

5.3. Poslední překážka

- Důkaz měl více než stovku stran a byl podroben přísnému zkoumání největších expertů v oboru.
- V srpnu 1993 objevil jeden z nich v důkaze mezeru, která se zprvu zdála jednoduše odstranitelná, ale postupně se ukázalo, že jde o vážnější problém.

5.3. Poslední překážka

- Důkaz měl více než stovku stran a byl podroben přísnému zkoumání největších expertů v oboru.
- V srpnu 1993 objevil jeden z nich v důkaze mezeru, která se zprvu zdála jednoduše odstranitelná, ale postupně se ukázalo, že jde o vážnější problém.
- Na odstranění chyby už nyní pracovala celá skupina expertů, především Richard Taylor.

5.3. Poslední překážka

- Důkaz měl více než stovku stran a byl podroben přísnému zkoumání největších expertů v oboru.
- V srpnu 1993 objevil jeden z nich v důkaze mezeru, která se zprvu zdála jednoduše odstranitelná, ale postupně se ukázalo, že jde o vážnější problém.
- Na odstranění chyby už nyní pracovala celá skupina expertů, především Richard Taylor. K zásadnímu průlomu došlo až v září 1994, ve chvíli, kdy už se Wiles chystal vzdát. . .

5.3. Poslední překážka

- Důkaz měl více než stovku stran a byl podroben přísnému zkoumání největších expertů v oboru.
- V srpnu 1993 objevil jeden z nich v důkaze mezeru, která se zprvu zdála jednoduše odstranitelná, ale postupně se ukázalo, že jde o vážnější problém.
- Na odstranění chyby už nyní pracovala celá skupina expertů, především Richard Taylor. K zásadnímu průlomu došlo až v září 1994, ve chvíli, kdy už se Wiles chystal vzdát...
- ...zjistil, že (Iwasavova) metoda, kterou kdysi opustil ve prospěch jiné, mu pomůže díru v důkazu zacelit.

5.3. Poslední překážka

- Důkaz měl více než stovku stran a byl podroben přísnému zkoumání největších expertů v oboru.
- V srpnu 1993 objevil jeden z nich v důkaze mezeru, která se zprvu zdála jednoduše odstranitelná, ale postupně se ukázalo, že jde o vážnější problém.
- Na odstranění chyby už nyní pracovala celá skupina expertů, především Richard Taylor. K zásadnímu průlomu došlo až v září 1994, ve chvíli, kdy už se Wiles chystal vzdát...
- ...zjistil, že (Iwasavova) metoda, kterou kdysi opustil ve prospěch jiné, mu pomůže díru v důkazu zacelit.
- Nechme promluvit samotného Andrew Wilese:

"Asi dvacet minut jsem zíral nevěřícně na stůl. Pak jsem celý den chodil po budově a vracel jsem se zpět ke svému stolu, abych se přesvědčil, že to tam stále ještě je. Bylo to tam. Nemohl jsem se ovládnout, tak jsem byl vzrušený. Byl to nejdůležitější okamžik mého pracovního života. Nic z toho, co kdy ještě udělám, nebude s tím srovnatelné."
(A. Wiles)

"Asi dvacet minut jsem zíral nevěřícně na stůl. Pak jsem celý den chodil po budově a vracel jsem se zpět ke svému stolu, abych se přesvědčil, že to tam stále ještě je. Bylo to tam. Nemohl jsem se ovládnout, tak jsem byl vzrušený. Byl to nejdůležitější okamžik mého pracovního života. Nic z toho, co kdy ještě udělám, nebude s tím srovnatelné."
(A. Wiles)

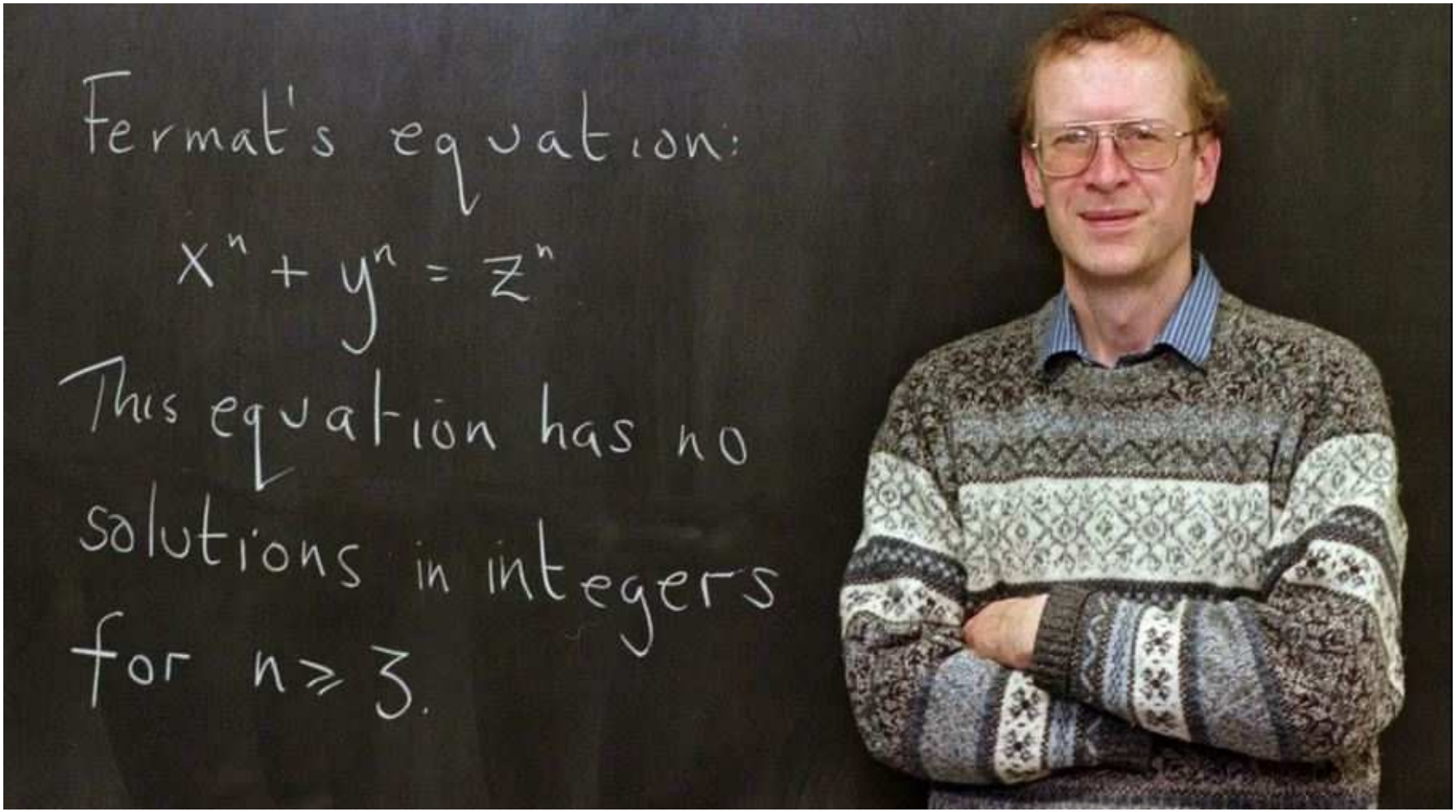
- 1995: byly publikovány dva články (A. Wiles, A. Wiles + R.Taylor)

"Asi dvacet minut jsem zíral nevěřícně na stůl. Pak jsem celý den chodil po budově a vracel jsem se zpět ke svému stolu, abych se přesvědčil, že to tam stále ještě je. Bylo to tam. Nemohl jsem se ovládnout, tak jsem byl vzrušený. Byl to nejdůležitější okamžik mého pracovního života. Nic z toho, co kdy ještě udělám, nebude s tím srovnatelné."
(A. Wiles)

- 1995: byly publikovány dva články (A. Wiles, A. Wiles + R.Taylor)
- Oba články dohromady dokazovaly mimo veškerou pochybnost T-S-W hypotézu pro tzv. semistabilní eliptické křivky, které zahrnují i hypotetickou Freyovu křivku.

"Asi dvacet minut jsem zíral nevěřícně na stůl. Pak jsem celý den chodil po budově a vracel jsem se zpět ke svému stolu, abych se přesvědčil, že to tam stále ještě je. Bylo to tam. Nemohl jsem se ovládnout, tak jsem byl vzrušený. Byl to nejdůležitější okamžik mého pracovního života. Nic z toho, co kdy ještě udělám, nebude s tím srovnatelné."
(A. Wiles)

- 1995: byly publikovány dva články (A. Wiles, A. Wiles + R.Taylor)
- Oba články dohromady dokazovaly mimo veškerou pochybnost T-S-W hypotézu pro tzv. semistabilní eliptické křivky, které zahrnují i hypotetickou Freyovu křivku. FLT byla dokázána.


Fermat's equation:
$x^n + y^n = z^n$
This equation has no solutions in integers for $n \geq 3$.

- **6.1. Byl Fermat neomylný?**

6.1. Byl Fermat neomylný?

Ne, někdy se spletl.

6.1. Byl Fermat neomylný?

Ne, někdy se spletl.Tzv. Fermatova čísla (pochopitelně studovaná Fermatem) jsou čísla tvaru $F_n := 2^{2^n} + 1$.

6.1. Byl Fermat neomylný?

Ne, někdy se spletl.Tzv. Fermatova čísla (pochopitelně studovaná Fermatem) jsou čísla tvaru $F_n := 2^{2^n} + 1$.
Fermatovo pozorování:

- $F_0 := 2^1 + 1 = 3$ je prvočíslo

6.1. Byl Fermat neomylný?

Ne, někdy se spletl.Tzv. Fermatova čísla (pochopitelně studovaná Fermatem) jsou čísla tvaru $F_n := 2^{2^n} + 1$.
Fermatovo pozorování:

- $F_0 := 2^1 + 1 = 3$ je prvočíslo
- $F_1 := 2^2 + 1 = 5$ je prvočíslo

6.1. Byl Fermat neomylný?

Ne, někdy se spletl.Tzv. Fermatova čísla (pochopitelně studovaná Fermatem) jsou čísla tvaru $F_n := 2^{2^n} + 1$.
Fermatovo pozorování:

- $F_0 := 2^1 + 1 = 3$ je prvočíslo
- $F_1 := 2^2 + 1 = 5$ je prvočíslo
- $F_2 := 2^4 + 1 = 17$ je prvočíslo

6.1. Byl Fermat neomylný?

Ne, někdy se spletl.Tzv. Fermatova čísla (pochopitelně studovaná Fermatem) jsou čísla tvaru $F_n := 2^{2^n} + 1$.
Fermatovo pozorování:

- $F_0 := 2^1 + 1 = 3$ je prvočíslo
- $F_1 := 2^2 + 1 = 5$ je prvočíslo
- $F_2 := 2^4 + 1 = 17$ je prvočíslo
- $F_3 := 2^8 + 1 = 257$ je prvočíslo

6.1. Byl Fermat neomylný?

Ne, někdy se spletl.Tzv. Fermatova čísla (pochopitelně studovaná Fermatem) jsou čísla tvaru $F_n := 2^{2^n} + 1$.
Fermatovo pozorování:

- $F_0 := 2^1 + 1 = 3$ je prvočíslo
- $F_1 := 2^2 + 1 = 5$ je prvočíslo
- $F_2 := 2^4 + 1 = 17$ je prvočíslo
- $F_3 := 2^8 + 1 = 257$ je prvočíslo
- $F_4 := 2^{16} + 1 = 65\,537$ je prvočíslo

6.1. Byl Fermat neomylný?

Ne, někdy se spletl.Tzv. Fermatova čísla (pochopitelně studovaná Fermatem) jsou čísla tvaru $F_n := 2^{2^n} + 1$.
Fermatovo pozorování:

- $F_0 := 2^1 + 1 = 3$ je prvočíslo
- $F_1 := 2^2 + 1 = 5$ je prvočíslo
- $F_2 := 2^4 + 1 = 17$ je prvočíslo
- $F_3 := 2^8 + 1 = 257$ je prvočíslo
- $F_4 := 2^{16} + 1 = 65\,537$ je prvočíslo

Fermat: "Všechna čísla tvaru $2^{2^n} + 1$ jsou prvočísla"

6.1. Byl Fermat neomylný?

Ne, někdy se spletl.Tzv. Fermatova čísla (pochopitelně studovaná Fermatem) jsou čísla tvaru $F_n := 2^{2^n} + 1$.
Fermatovo pozorování:

- $F_0 := 2^1 + 1 = 3$ je prvočíslo
- $F_1 := 2^2 + 1 = 5$ je prvočíslo
- $F_2 := 2^4 + 1 = 17$ je prvočíslo
- $F_3 := 2^8 + 1 = 257$ je prvočíslo
- $F_4 := 2^{16} + 1 = 65\,537$ je prvočíslo

Fermat: "Všechna čísla tvaru $2^{2^n} + 1$ jsou prvočísla"

Leonhard Euler v r. 1732: Nikoli,

$$F_5 := 2^{32} + 1 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417$$

6.1. Byl Fermat neomylný?

Ne, někdy se spletl.Tzv. Fermatova čísla (pochopitelně studovaná Fermatem) jsou čísla tvaru $F_n := 2^{2^n} + 1$.
Fermatovo pozorování:

- $F_0 := 2^1 + 1 = 3$ je prvočíslo
- $F_1 := 2^2 + 1 = 5$ je prvočíslo
- $F_2 := 2^4 + 1 = 17$ je prvočíslo
- $F_3 := 2^8 + 1 = 257$ je prvočíslo
- $F_4 := 2^{16} + 1 = 65\,537$ je prvočíslo

Fermat: "Všechna čísla tvaru $2^{2^n} + 1$ jsou prvočísla"

Leonhard Euler v r. 1732: Nikoli,

$$F_5 := 2^{32} + 1 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417$$

Dnes víme, že všechna čísla F_5 až F_{32} jsou složená. A dál už na to nestačíme (F_{32} má cca miliardu cifer).

6.2. Racionální body na jistých křivkách

6.2. Racionální body na jistých křivkách

Pokud platí

$$p^n + q^n = r^n \qquad \text{pro nějaká} \quad p, q, r \in \mathbb{N}$$

6.2. Racionální body na jistých křivkách

Pokud platí

$$p^n + q^n = r^n \qquad \text{pro nějaká} \quad p, q, r \in \mathbb{N}$$

pak platí i $\left(\frac{p}{r}\right)^n + \left(\frac{q}{r}\right)^n = 1$

6.2. Racionální body na jistých křivkách

Pokud platí

$$p^n + q^n = r^n \qquad \text{pro nějaká} \quad p, q, r \in \mathbb{N}$$

pak platí i $\left(\frac{p}{r}\right)^n + \left(\frac{q}{r}\right)^n = 1$ pro nějaká $p, q, r \in \mathbb{N}$,

6.2. Racionální body na jistých křivkách

Pokud platí

$$p^n + q^n = r^n \qquad \text{pro nějaká} \quad p, q, r \in \mathbb{N}$$

pak platí i $\left(\frac{p}{r}\right)^n + \left(\frac{q}{r}\right)^n = 1$ pro nějaká $p, q, r \in \mathbb{N}$, a tedy

$$x^n + y^n = 1 \qquad \text{pro nějaká} \quad x, y \in \mathbb{Q}.$$

6.2. Racionální body na jistých křivkách

Pokud platí

$$p^n + q^n = r^n \qquad \text{pro nějaká} \quad p, q, r \in \mathbb{N}$$

pak platí i $\left(\frac{p}{r}\right)^n + \left(\frac{q}{r}\right)^n = 1$ pro nějaká $p, q, r \in \mathbb{N}$, a tedy

$$x^n + y^n = 1 \qquad \text{pro nějaká} \quad x, y \in \mathbb{Q}.$$

A naopak:

6.2. Racionální body na jistých křivkách

Pokud platí

$$p^n + q^n = r^n \qquad \text{pro nějaká} \quad p, q, r \in \mathbb{N}$$

pak platí i $\left(\frac{p}{r}\right)^n + \left(\frac{q}{r}\right)^n = 1$ pro nějaká $p, q, r \in \mathbb{N}$, a tedy

$$x^n + y^n = 1 \qquad \text{pro nějaká} \quad x, y \in \mathbb{Q}.$$

A naopak: $\left(\frac{p}{r}\right)^n + \left(\frac{q}{s}\right)^n = 1$

6.2. Racionální body na jistých křivkách

Pokud platí

$$p^n + q^n = r^n \qquad \text{pro nějaká} \quad p, q, r \in \mathbb{N}$$

pak platí i $\left(\frac{p}{r}\right)^n + \left(\frac{q}{r}\right)^n = 1$ pro nějaká $p, q, r \in \mathbb{N}$, a tedy

$$x^n + y^n = 1 \qquad \text{pro nějaká} \quad x, y \in \mathbb{Q}.$$

A naopak: $\left(\frac{p}{r}\right)^n + \left(\frac{q}{s}\right)^n = 1 \implies (ps)^n + (qr)^n = (rs)^n$.

6.2. Racionální body na jistých křivkách

Pokud platí

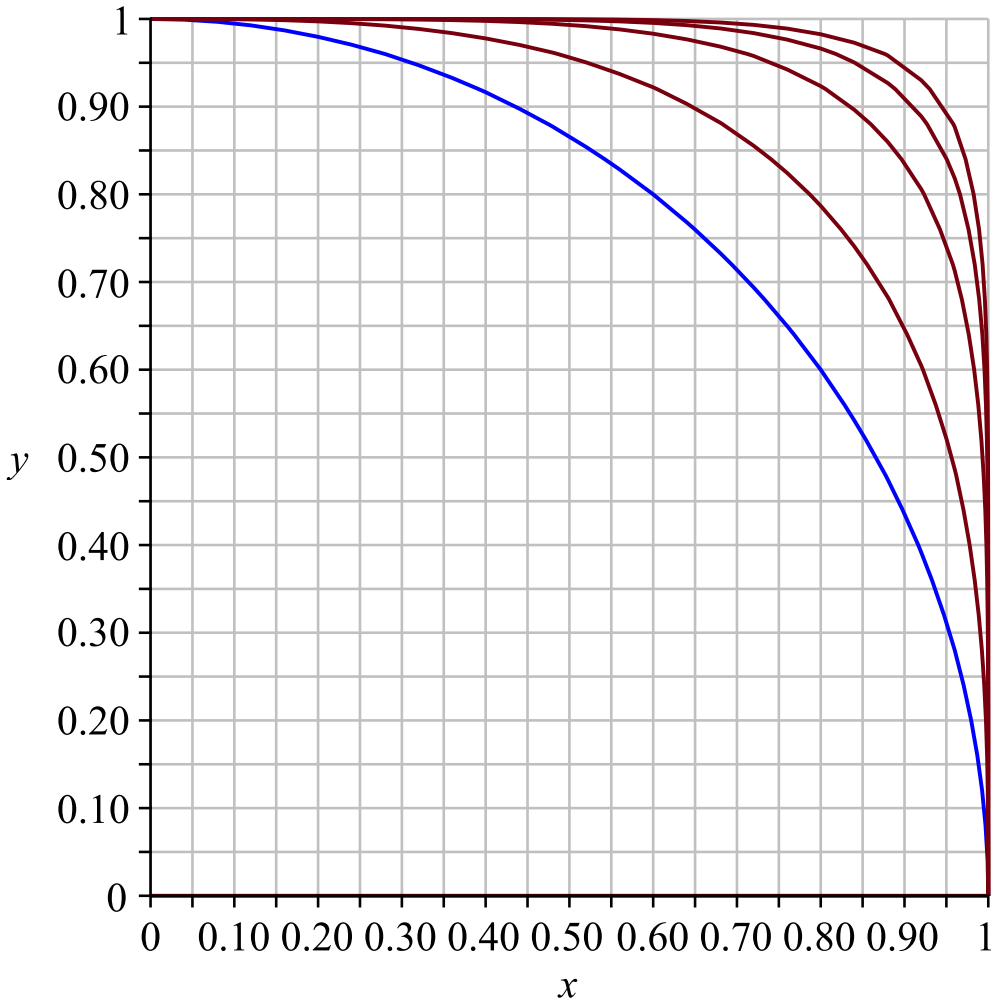
$$p^n + q^n = r^n \qquad \text{pro nějaká} \quad p, q, r \in \mathbb{N}$$

pak platí i $\left(\frac{p}{r}\right)^n + \left(\frac{q}{r}\right)^n = 1$ pro nějaká $p, q, r \in \mathbb{N}$, a tedy

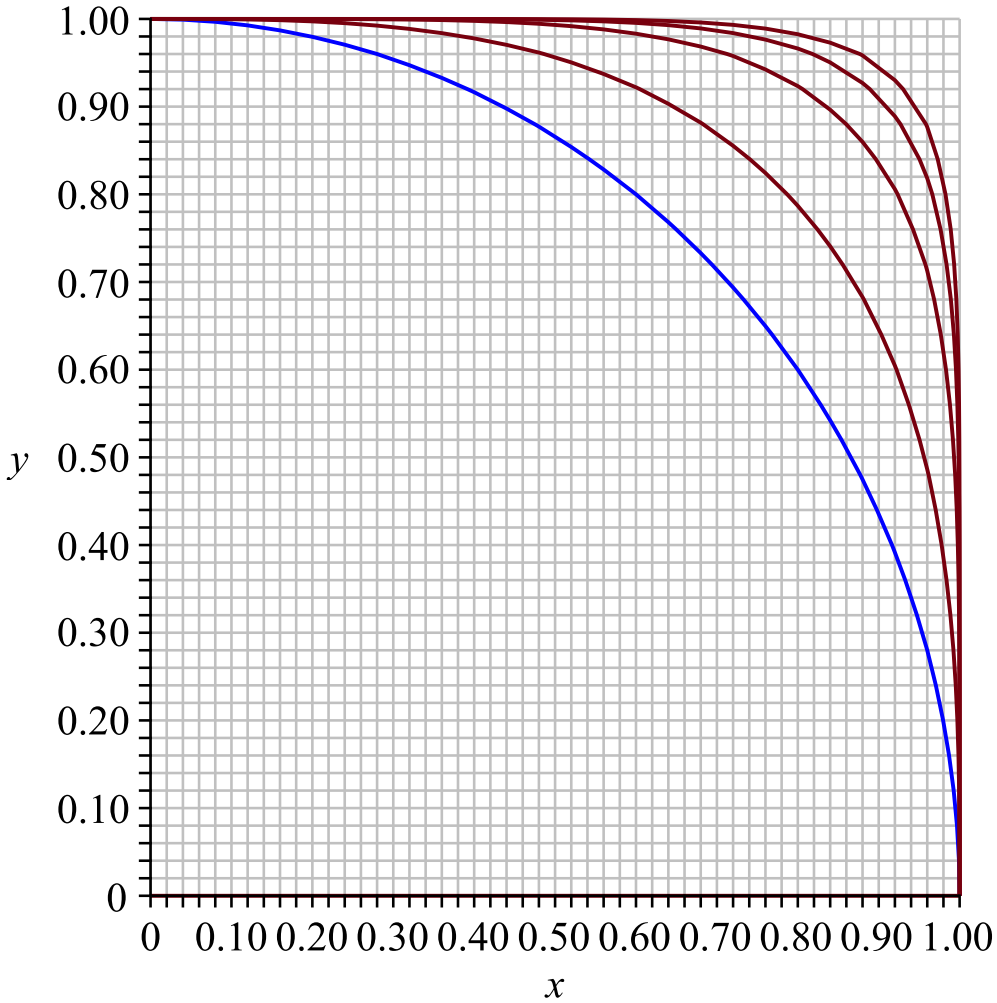
$$x^n + y^n = 1 \qquad \text{pro nějaká} \quad x, y \in \mathbb{Q}.$$

A naopak: $\left(\frac{p}{r}\right)^n + \left(\frac{q}{s}\right)^n = 1 \implies (ps)^n + (qr)^n = (rs)^n$.

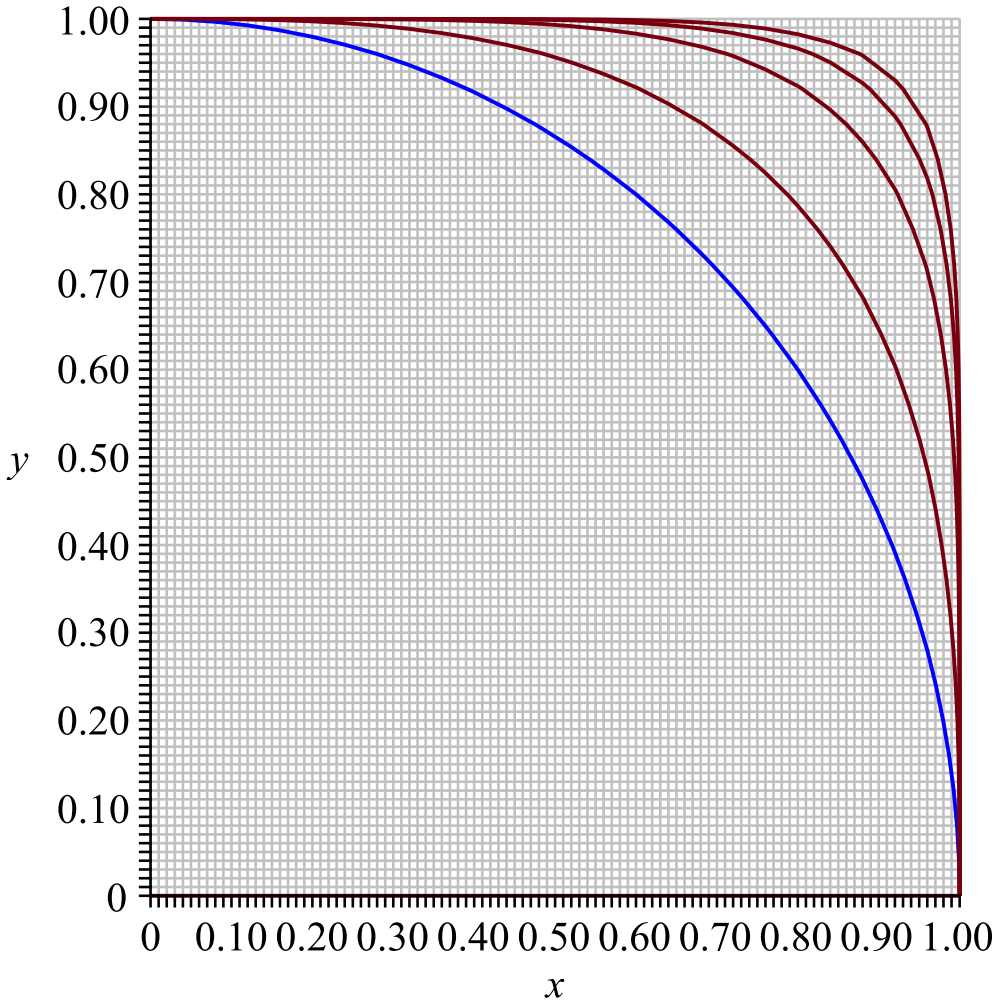
Existence řešení Fermatovy rovnice $x^n + y^n = z^n$ je tedy ekvivalentní existenci racionálních bodů na křivce $x^n + y^n = 1$.



$$x^2 + y^2 = 1, \qquad x^k + y^k = 1 \text{ pro } k = 3, 5, 7, 9$$



$$x^2 + y^2 = 1, \quad x^k + y^k = 1 \text{ pro } k = 3, 5, 7, 9$$



$$x^2 + y^2 = 1, \qquad x^k + y^k = 1 \text{ pro } k = 3, 5, 7, 9$$

6.3. Má FLT nějaké využití, je důležitá?

- **6.3. Má FLT nějaké využití, je důležitá?**
- Gauss měl pravdu: Ani ne, je to izolované tvrzení bez důležitých důsledků.

- **6.3. Má FLT nějaké využití, je důležitá?**
- Gauss měl pravdu: Ani ne, je to izolované tvrzení bez důležitých důsledků. (Snad jen. . .

6.3. Má FLT nějaké využití, je důležitá?

- Gauss měl pravdu: Ani ne, je to izolované tvrzení bez důležitých důsledků. (Snad jen. . . "bouchalovský" důkaz iracionality $\sqrt[k]{2}$ pro $k > 2$.)

- **6.3. Má FLT nějaké využití, je důležitá?**
- Gauss měl pravdu: Ani ne, je to izolované tvrzení bez důležitých důsledků. (Snad jen. . . "bouchalovský" důkaz iracionality $\sqrt[k]{2}$ pro $k > 2$.)

Nicméně:

6.3. Má FLT nějaké využití, je důležitá?

- Gauss měl pravdu: Ani ne, je to izolované tvrzení bez důležitých důsledků. (Snad jen. . . "bouchalovský" důkaz iracionality $\sqrt[k]{2}$ pro $k > 2$.)

Nicméně:

> Cesta za hledáním důkazu FLT přinesla neuvěřitelné množství hlubokých poznatků z teorie čísel, které samy o sobě mají obrovský význam.

6.3. Má FLT nějaké využití, je důležitá?

- Gauss měl pravdu: Ani ne, je to izolované tvrzení bez důležitých důsledků. (Snad jen. . . "bouchalovský" důkaz iracionality $\sqrt[k]{2}$ pro $k > 2$.)

Nicméně:

> Cesta za hledáním důkazu FLT přinesla neuvěřitelné množství hlubokých poznatků z teorie čísel, které samy o sobě mají obrovský význam.

Úsilí, trvající více než 350 let vedlo nakonec k cíli.

6.3. Má FLT nějaké využití, je důležitá?

- Gauss měl pravdu: Ani ne, je to izolované tvrzení bez důležitých důsledků. (Snad jen. . . "bouchalovský" důkaz iracionality $\sqrt[k]{2}$ pro $k > 2$.)

Nicméně:

> Cesta za hledáním důkazu FLT přinesla neuvěřitelné množství hlubokých poznatků z teorie čísel, které samy o sobě mají obrovský význam.

Úsilí, trvající více než 350 let vedlo nakonec k cíli.

Člověk by se neměl vzdávat, i když mu to třeba někdy nemyslí:

„Pan profesor tady sedí už od rána, ale zdá se,
že dnes není větru v mlýnech jeho mysli."

I think I'll stop here.

Mirko Rokyta
KMA MFF Praha
Sokolovská 83
Praha 8 - Karlín

mirko.rokyta@mff.cuni.cz