

# Pohstův prvočíselný problém a aritmetické posloupnosti

Zuzana Masáková

Podle článku:

L. Hajdu, *Arithmetic Progressions in Linear Combinations of  $S$ -units*, *Period. Math. Hung.* **54** (2007), 5161.

15. listopadu 2011

## Pohstův problém

M. Pohst (TU Berlin) :

Je možné zapsat libovolné prvočíslo  $p$  ve tvaru  $p = 2^u \pm 3^v$ ,

$u, v \in \mathbb{N}_0$ ?

$$2 =$$

## Pohstův problém

M. Pohst (TU Berlin) :

Je možné zapsat libovolné prvočíslo  $p$  ve tvaru  $p = 2^u \pm 3^v$ ,

$u, v \in \mathbb{N}_0$ ?

$$2 = 2^0 + 3^0$$

$$3 =$$

## Pohstův problém

M. Pohst (TU Berlin) :

Je možné zapsat libovolné prvočíslo  $p$  ve tvaru  $p = 2^u \pm 3^v$ ,

$u, v \in \mathbb{N}_0$ ?

$$2 = 2^0 + 3^0$$

$$3 = 2^1 + 3^0$$

$$5 =$$

## Pohstův problém

M. Pohst (TU Berlin) :

Je možné zapsat libovolné prvočíslo  $p$  ve tvaru  $p = 2^u \pm 3^v$ ,

$u, v \in \mathbb{N}_0$ ?

$$2 = 2^0 + 3^0$$

$$3 = 2^1 + 3^0$$

$$5 = 2^1 + 3^1$$

$$7 =$$

## Pohstův problém

M. Pohst (TU Berlin) :

Je možné zapsat libovolné prvočíslo  $p$  ve tvaru  $p = 2^u \pm 3^v$ ,  
 $u, v \in \mathbb{N}_0$ ?

$$2 = 2^0 + 3^0$$

$$3 = 2^1 + 3^0$$

$$5 = 2^1 + 3^1$$

$$7 = 2^2 + 3^1$$

$$11 =$$

## Pohstův problém

M. Pohst (TU Berlin) :

Je možné zapsat libovolné prvočíslo  $p$  ve tvaru  $p = 2^u \pm 3^v$ ,  
 $u, v \in \mathbb{N}_0$ ?

$$2 = 2^0 + 3^0$$

$$3 = 2^1 + 3^0$$

$$5 = 2^1 + 3^1$$

$$7 = 2^2 + 3^1$$

$$11 = 2^1 + 3^2$$

$$13 =$$

## Pohstův problém

M. Pohst (TU Berlin) :

Je možné zapsat libovolné prvočíslo  $p$  ve tvaru  $p = 2^u \pm 3^v$ ,  
 $u, v \in \mathbb{N}_0$ ?

$$2 = 2^0 + 3^0$$

$$3 = 2^1 + 3^0$$

$$5 = 2^1 + 3^1$$

$$7 = 2^2 + 3^1$$

$$11 = 2^1 + 3^2$$

$$13 = 2^2 + 3^2$$



## Pohstův problém

M. Pohst (TU Berlin) :

Je možné zapsat libovolné prvočíslo  $p$  ve tvaru  $p = 2^u \pm 3^v$ ,  
 $u, v \in \mathbb{N}_0$ ?

$$2 = 2^0 + 3^0$$

$$3 = 2^1 + 3^0$$

$$5 = 2^1 + 3^1$$

$$7 = 2^2 + 3^1$$

$$11 = 2^1 + 3^2$$

$$13 = 2^2 + 3^2 = 2^8 - 3^5$$

$$17 =$$

## Pohstův problém

M. Pohst (TU Berlin) :

Je možné zapsat libovolné prvočíslo  $p$  ve tvaru  $p = 2^u \pm 3^v$ ,  
 $u, v \in \mathbb{N}_0$ ?

$$2 = 2^0 + 3^0$$

$$3 = 2^1 + 3^0$$

$$5 = 2^1 + 3^1$$

$$7 = 2^2 + 3^1$$

$$11 = 2^1 + 3^2$$

$$13 = 2^2 + 3^2 = 2^8 - 3^5$$

$$17 = 2^3 + 3^2 = 2^4 + 3^2$$

$$19 =$$

## Pohstův problém

M. Pohst (TU Berlin) :

Je možné zapsat libovolné prvočíslo  $p$  ve tvaru  $p = 2^u \pm 3^v$ ,  
 $u, v \in \mathbb{N}_0$ ?

$$2 = 2^0 + 3^0$$

$$3 = 2^1 + 3^0$$

$$5 = 2^1 + 3^1$$

$$7 = 2^2 + 3^1$$

$$11 = 2^1 + 3^2$$

$$13 = 2^2 + 3^2 = 2^8 - 3^5$$

$$17 = 2^3 + 3^2 = 2^4 + 3^2$$

$$19 = 2^4 + 3^1$$

$$23 =$$

## Pohstův problém

M. Pohst (TU Berlin) :

Je možné zapsat libovolné prvočíslo  $p$  ve tvaru  $p = 2^u \pm 3^v$ ,  
 $u, v \in \mathbb{N}_0$ ?

$$2 = 2^0 + 3^0$$

$$3 = 2^1 + 3^0$$

$$5 = 2^1 + 3^1$$

$$7 = 2^2 + 3^1$$

$$11 = 2^1 + 3^2$$

$$13 = 2^2 + 3^2 = 2^8 - 3^5$$

$$17 = 2^3 + 3^2 = 2^4 + 3^2$$

$$19 = 2^4 + 3^1$$

$$23 = 2^5 - 3^2$$

⋮

## Značení

$K$  algebraicky uzavřené těleso charakteristiky 0 (má prvotěleso  $\mathbb{Q}$ )

## Značení

$K$  algebraicky uzavřené těleso charakteristiky 0 (má prvotěleso  $\mathbb{Q}$ )  
 $\Gamma$  multiplikatívni podgrupa  $K^*$  konečného ranku  $r$

# Značení

$K$  algebraicky uzavřené těleso charakteristiky 0 (má prvotěleso  $\mathbb{Q}$ )  
 $\Gamma$  multiplikativní podgrupa  $K^*$  konečného ranku  $r$

**Příklady:**

$$\Gamma = \{\pm 1\},$$

# Značení

$K$  algebraicky uzavřené těleso charakteristiky 0 (má prvotěleso  $\mathbb{Q}$ )  
 $\Gamma$  multiplikatívni podgrupa  $K^*$  konečného ranku  $r$

**Příklady:**

$$\Gamma = \{\pm 1\}, \quad \Gamma = \{\pm \tau^k \mid k \in \mathbb{Z}\},$$



# Značení

$K$  algebraicky uzavřené těleso charakteristiky 0 (má prvotěleso  $\mathbb{Q}$ )  
 $\Gamma$  multiplikativní podgrupa  $K^*$  konečného ranku  $r$

**Příklady:**

$$\Gamma = \{\pm 1\}, \quad \Gamma = \{\pm \tau^k \mid k \in \mathbb{Z}\}, \quad \Gamma = \{2^k \mid k \in \mathbb{Z}\},$$

# Značení

$K$  algebraicky uzavřené těleso charakteristiky 0 (má prvotěleso  $\mathbb{Q}$ )  
 $\Gamma$  multiplikativní podgrupa  $K^*$  konečného ranku  $r$

## Příklady:

$$\Gamma = \{\pm 1\}, \quad \Gamma = \{\pm \tau^k \mid k \in \mathbb{Z}\}, \quad \Gamma = \{2^k \mid k \in \mathbb{Z}\},$$

$S$  neprázdná konečná množina prvočísel,

$$\mathbb{Z}_S = \{m \in \mathbb{Z} \mid p \text{ prvočíslo, } p|m \Rightarrow p \in S\},$$

$$\Gamma = U_S = \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z} \setminus 0, p \perp q, pq \in \mathbb{Z}_S \right\}.$$

# Značení

$K$  algebraicky uzavřené těleso charakteristiky 0 (má prvotěleso  $\mathbb{Q}$ )  
 $\Gamma$  multiplikativní podgrupa  $K^*$  konečného ranku  $r$

**Příklady:**

$$\Gamma = \{\pm 1\}, \quad \Gamma = \{\pm \tau^k \mid k \in \mathbb{Z}\}, \quad \Gamma = \{2^k \mid k \in \mathbb{Z}\},$$

$S$  neprázdňá konečňá množina prvočísel,

$$\mathbb{Z}_S = \{m \in \mathbb{Z} \mid p \text{ prvočíslo, } p|m \Rightarrow p \in S\},$$

$$\Gamma = U_S = \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z} \setminus 0, p \perp q, pq \in \mathbb{Z}_S \right\}.$$

$t \in \mathbb{N}$ ,  $\mathcal{A}$  neprázdňá konečňá podmnožina  $K^t$

$$H_t(\Gamma, \mathcal{A}) = \left\{ \sum_{i=1}^t a_i x_i \mid (a_1, \dots, a_t) \in \mathcal{A}, (x_1, \dots, x_t) \in \Gamma^t \right\}.$$

## Věta první

$K$  algebraicky uzavřené těleso charakteristiky 0

$\Gamma$  multiplikativní podgrupa  $K^*$  konečného ranku  $r$

$t \in \mathbb{N}$ ,  $\mathcal{A}$  podmnožina  $K^t$  o  $n$  prvcích

$$H_t(\Gamma, \mathcal{A}) = \left\{ \sum_{i=1}^t a_i x_i \mid (a_1, \dots, a_t) \in \mathcal{A}, (x_1, \dots, x_t) \in \Gamma^t \right\}.$$

## Věta první

$K$  algebraicky uzavřené těleso charakteristiky 0

$\Gamma$  multiplikativní podgrupa  $K^*$  konečného ranku  $r$

$t \in \mathbb{N}$ ,  $\mathcal{A}$  podmnožina  $K^t$  o  $n$  prvcích

$$H_t(\Gamma, \mathcal{A}) = \left\{ \sum_{i=1}^t a_i x_i \mid (a_1, \dots, a_t) \in \mathcal{A}, (x_1, \dots, x_t) \in \Gamma^t \right\}.$$

## Věta (Hajdu 2006)

*Pro každé  $r, t, n$  existuje  $C(r, t, n)$  tak, že pro každou podgrupu  $\Gamma$  ranku  $r$  a každou  $n$ -prvkovou abecedu  $\mathcal{A}$  délka každé nekonstantní aritmetické posloupnosti v  $H_t(\Gamma, \mathcal{A})$  je omezena konstantou  $C(r, t, n)$ .*

## První poznámka k první větě

Závislost konstanty  $C(r, t, n)$  na  $r, t, n$  nelze vynechat:

## První poznámka k první větě

Závislost konstanty  $C(r, t, n)$  na  $r, t, n$  nelze vynechat:

### Příklad 1:

$t$  pevné,  $\Gamma = \{-1, 1\}$ ,  $\mathcal{A} = \{(1, \dots, 1)\}$ ,

$$H_t(\Gamma, \mathcal{A}) = \left\{ \sum_{i=1}^t x_i \mid x_i \in \{-1, 1\} \right\}$$

obsahuje aritmetickou posloupnost délky  $t + 1$ :

$$\begin{aligned} -t &= (-1) + (-1) + \dots + (-1) + (-1) \\ -t + 2 &= 1 + (-1) + \dots + (-1) + (-1) \\ &\vdots \\ t - 2 &= 1 + 1 + \dots + 1 + (-1) \\ t &= 1 + 1 + \dots + 1 + 1 \end{aligned}$$

## První poznámka k první větě

Závislost konstanty  $C(r, t, n)$  na  $r, t, n$  nelze vynechat:

### Příklad 2:

$$t = 1, \Gamma = \{1\}, \mathcal{A} = \{1, 2, \dots, n\},$$

$$H_1(\Gamma, \mathcal{A}) = \left\{ \sum_{i=1}^1 a_i \mid a_i \in \mathcal{A} \right\} = \mathcal{A}$$

obsahuje aritmetickou posloupnost  $1, 2, \dots, n$  délky  $n$ .



## První poznámka k první větě

Závislost konstanty  $C(r, t, n)$  na  $r, t, n$  nelze vynechat:

### Příklad 3:

$t = 1, \mathcal{A} = \{1\},$

pro pevné  $k \in \mathbb{N}, k \geq 2$ , vezmi  $S = \{p \mid p \text{ je prvočíslo, } p|k!\}$

$\Gamma = U_S$ , rank  $\Gamma$  je  $r = |S| + 1 = \pi(k) + 1$ .

$$H_1(\Gamma, \mathcal{A}) = \left\{ \sum_{i=1}^1 x_i \mid x_i \in U_S \right\} = U_S$$

obsahuje aritm. posloupnost  $1, 2, \dots, k$  délky  $k$  (závislost na  $r$ ).

## Druhá poznámka k první větě

Počet aritmetických posloupností v  $H_t(\Gamma, S)$  není omezený:

## Druhá poznámka k první větě

Počet aritmetických posloupností v  $H_t(\Gamma, S)$  není omezený:

### Příklad 1:

$t = 1$ ,  $\Gamma = U_S$  pro  $S = \{2\}$ ,  $\mathcal{A} = \{0, 1\}$ ,

$$H_1(\Gamma, \mathcal{A}) = \{ax \mid a \in \{0, 1\}, x \in \Gamma_S\} = U_S \cup \{0\}$$

obsahuje aritmetickou posloupnost  $0, 2^u, 2^{u+1}$  pro každé  $u \in \mathbb{N}_0$ .

## Druhá poznámka k první větě

Počet aritmetických posloupností v  $H_t(\Gamma, S)$  není omezený:

### Příklad 1:

$t = 1$ ,  $\Gamma = U_S$  pro  $S = \{2\}$ ,  $\mathcal{A} = \{0, 1\}$ ,

$$H_1(\Gamma, \mathcal{A}) = \{ax \mid a \in \{0, 1\}, x \in \Gamma_S\} = U_S \cup \{0\}$$

obsahuje aritmetickou posloupnost  $0, 2^u, 2^{u+1}$  pro každé  $u \in \mathbb{N}_0$ .

### Příklad 2:

$t = 2$ ,  $\mathcal{A}' = \{(0, 1), (1, 1)\}$ ,

$$1, 2^u + 1, 2^{u+1} + 1, \quad u \in \mathbb{N}_0,$$

je aritmetická posloupnost v  $H_2(\Gamma, \mathcal{A}')$ .

## Druhá poznámka k první větě

Počet aritmetických posloupností v  $H_t(\Gamma, S)$  není omezený:

### Obecně:

Když  $q_1, \dots, q_l$  je aritmetická posloupnost v  $H_t(\Gamma, \mathcal{A})$ ,  
pak  $q_1 + x, \dots, q_l + x$  je pro každé  $x \in \Gamma$  aritmetická  
posloupnost v  $H_{t+1}(\Gamma, \mathcal{A}')$  pro vhodnou  $\mathcal{A}'$ .

## Druhá poznámka k první větě

Počet aritmetických posloupností v  $H_t(\Gamma, S)$  není omezený:

### Obecně:

Když  $q_1, \dots, q_l$  je aritmetická posloupnost v  $H_t(\Gamma, \mathcal{A})$ ,  
pak  $q_1 + x, \dots, q_l + x$  je pro každé  $x \in \Gamma$  aritmetická  
posloupnost v  $H_{t+1}(\Gamma, \mathcal{A}')$  pro vhodnou  $\mathcal{A}'$ .

Obecně může  $H_t(\Gamma, \mathcal{A})$  obsahovat nekonečně mnoho aritmetických  
posloupností.

## Věta druhá

### Věta (Green and Tao 2004)

*Existují libovolně dlouhé aritmetické posloupnosti prvočísel.*

# Věta druhá

## Věta (Green and Tao 2004)

*Existují libovolně dlouhé aritmetické posloupnosti prvočísel.*

Pro zajímavost:

## Věta (Tao and Ziegler 2006)

*Pro libovolné  $k \in \mathbb{N}$  a polynomy  $P_1, \dots, P_k \in \mathbb{Z}[x]$ ,  $P_i(0) = 0$ , existuje nekonečně mnoho  $a, m \in \mathbb{Z}$  tak, že*

$$a + P_1(m), \dots, a + P_k(m)$$

*jsou prvočísla.*



# Věta druhá

## Věta (Green and Tao 2004)

*Existují libovolně dlouhé aritmetické posloupnosti prvočísel.*

Pro zajímavost:

## Věta (Tao and Ziegler 2006)

*Pro libovolné  $k \in \mathbb{N}$  a polynomy  $P_1, \dots, P_k \in \mathbb{Z}[x]$ ,  $P_i(0) = 0$ , existuje nekonečně mnoho  $a, m \in \mathbb{Z}$  tak, že*

$$a + P_1(m), \dots, a + P_k(m)$$

*jsou prvočísla.*

Dává Greenovu–Taovu větu pro

$$P_1(m) = m, P_2(m) = 2m, \dots, P_k(m) = km.$$

# Věta druhá

## Věta (Green and Tao 2004)

*Existují libovolně dlouhé aritmetické posloupnosti prvočísel.*

Pro zajímavost:

Nejdelší známá aritmetická posloupnost prvočísel - **délky 26**

$$43\ 142\ 746\ 595\ 714\ 191 \quad + \quad 23\ 681\ 770 \cdot 223\ 092\ 870 \ j,$$

pro  $j = 0, \dots, 25$ . Pozn.

$$223\ 092\ 870 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23.$$

(Projekt PrimeGrid - Perichaud 2010)

## Věta třetí

### Věta (Hajdu 2006)

Pro každé  $S = \{p_1, \dots, p_s\}$ ,  $t \in \mathbb{N}$  a  $\mathcal{A} \subset \mathbb{Z}^t$  existuje nekonečně mnoho prvočísel mimo množinu

$$H_t(\mathbb{Z}_S, \mathcal{A}) := \left\{ \sum_{i=1}^t a_i s_i \mid (a_1, \dots, a_t) \in \mathcal{A}, (s_1, \dots, s_t) \in \mathbb{Z}_S^t \right\}.$$

## Věta třetí

### Věta (Hajdu 2006)

Pro každé  $S = \{p_1, \dots, p_s\}$ ,  $t \in \mathbb{N}$  a  $\mathcal{A} \subset \mathbb{Z}^t$  existuje nekonečně mnoho prvočísel mimo množinu

$$H_t(\mathbb{Z}_S, \mathcal{A}) := \left\{ \sum_{i=1}^t a_i s_i \mid (a_1, \dots, a_t) \in \mathcal{A}, (s_1, \dots, s_t) \in \mathbb{Z}_S^t \right\}.$$

### Důkaz

$t \in \mathbb{N}$ ,  $\mathbb{Z}_S \subset \Gamma = U_S$ , rank  $\Gamma$  je  $r = |S| + 1$ ,  $\mathcal{A} \subset \mathbb{Z}^t$ ,  $|\mathcal{A}| = n$ .

## Věta třetí

### Věta (Hajdu 2006)

Pro každé  $S = \{p_1, \dots, p_s\}$ ,  $t \in \mathbb{N}$  a  $\mathcal{A} \subset \mathbb{Z}^t$  existuje nekonečně mnoho prvočísel mimo množinu

$$H_t(\mathbb{Z}_S, \mathcal{A}) := \left\{ \sum_{i=1}^t a_i s_i \mid (a_1, \dots, a_t) \in \mathcal{A}, (s_1, \dots, s_t) \in \mathbb{Z}_S^t \right\}.$$

### Důkaz

$t \in \mathbb{N}$ ,  $\mathbb{Z}_S \subset \Gamma = U_S$ , rank  $\Gamma$  je  $r = |S| + 1$ ,  $\mathcal{A} \subset \mathbb{Z}^t$ ,  $|\mathcal{A}| = n$ .

Z Greenovy-Taovy věty existuje nekonečně mnoho po dvou disjunktních aritmetických posloupností délky  $C(r, t, n) + 1$ .

## Věta třetí

### Věta (Hajdu 2006)

Pro každé  $S = \{p_1, \dots, p_s\}$ ,  $t \in \mathbb{N}$  a  $\mathcal{A} \subset \mathbb{Z}^t$  existuje nekonečně mnoho prvočísel mimo množinu

$$H_t(\mathbb{Z}_S, \mathcal{A}) := \left\{ \sum_{i=1}^t a_i s_i \mid (a_1, \dots, a_t) \in \mathcal{A}, (s_1, \dots, s_t) \in \mathbb{Z}_S^t \right\}.$$

### Důkaz

$t \in \mathbb{N}$ ,  $\mathbb{Z}_S \subset \Gamma = U_S$ , rank  $\Gamma$  je  $r = |S| + 1$ ,  $\mathcal{A} \subset \mathbb{Z}^t$ ,  $|\mathcal{A}| = n$ .

Z Greenovy-Taovy věty existuje nekonečně mnoho po dvou disjunktních aritmetických posloupností délky  $C(r, t, n) + 1$ .

Podle věty první v každé z nich musí být alespoň jedno prvočíslu mimo  $H_t(U_S, \mathcal{A}) \supset H_t(\mathbb{Z}_S, \mathcal{A})$ .

## Věta třetí

### Věta (Hajdu 2006)

Pro každé  $S = \{p_1, \dots, p_r\}$ ,  $t \in \mathbb{N}$  a  $\mathcal{A} \subset \mathbb{Z}^t$  existuje nekonečně mnoho prvočísel mimo množinu

$$H_t(\mathbb{Z}_S, \mathcal{A}) := \left\{ \sum_{i=1}^t a_i s_i \mid (a_1, \dots, a_t) \in \mathcal{A}, (s_1, \dots, s_t) \in \mathbb{Z}_S^t \right\}.$$

## Věta třetí

### Věta (Hajdu 2006)

Pro každé  $S = \{p_1, \dots, p_r\}$ ,  $t \in \mathbb{N}$  a  $\mathcal{A} \subset \mathbb{Z}^t$  existuje nekonečně mnoho prvočísel mimo množinu

$$H_t(\mathbb{Z}_S, \mathcal{A}) := \left\{ \sum_{i=1}^t a_i s_i \mid (a_1, \dots, a_t) \in \mathcal{A}, (s_1, \dots, s_t) \in \mathbb{Z}_S^t \right\}.$$

### Pozn.

Mersennova prvočísla tvaru  $2^u - 1$ ,  $u \in \mathbb{N}$ , patří do  $H_2(\mathbb{Z}_S, \mathcal{A})$ .

Věří se, že těch je nekonečně mnoho.

Obecně tedy asi nelze vylepšit na  $|H_t(\mathbb{Z}_S, \mathcal{A})| < +\infty$ .



# Řešení Pohstova problému

## Věta (Hajdu 2006)

Pro každé  $S = \{p_1, \dots, p_r\}$ ,  $t \in \mathbb{N}$  a  $\mathcal{A} \subset \mathbb{Z}^t$  existuje nekonečně mnoho prvočísel mimo množinu

$$H_t(\mathbb{Z}_S, \mathcal{A}) := \left\{ \sum_{i=1}^t a_i s_i \mid (a_1, \dots, a_t) \in \mathcal{A}, (s_1, \dots, s_t) \in \mathbb{Z}_S^t \right\}.$$

Vezmi  $S = \{2, 3\}$ ,  $t = 2$ ,  $\mathcal{A} = \{(1, 1)\}$ . Pak

$$H_2(\mathbb{Z}_S, \mathcal{A}) = \{\pm 2^i 3^j \pm 2^k 3^l \mid i, j, k, l \in \mathbb{N}_0\} \supset \{2^u \pm 3^v \mid u, v \in \mathbb{N}_0\}.$$

## Řešení Pohstova problému

M. Pohst (TU Berlin) :

Je možné zapsat libovolné prvočíslo  $p$  ve tvaru  $p = 2^u \pm 3^v$ ,

$u, v \in \mathbb{N}_0$ ?

**NE!**

# Řešení Pohstova problému

M. Pohst (TU Berlin) :

Je možné zapsat libovolné prvočíslo  $p$  ve tvaru  $p = 2^u \pm 3^v$ ,  
 $u, v \in \mathbb{N}_0$ ?

**NE!**

$$2 = 2^0 + 3^0$$

$$23 = 2^5 - 3^2$$

$$3 = 2^1 + 3^0$$

$$29 = 2^1 + 3^3$$

$$5 = 2^1 + 3^1$$

$$31 = 2^2 + 3^3$$

$$7 = 2^2 + 3^1$$

$$37 = 2^6 - 3^3$$

$$11 = 2^1 + 3^2$$

$$41 = 2^5 + 3^2$$

$$13 = 2^2 + 3^2$$

$$43 = 2^4 + 3^3$$

$$17 = 2^3 + 3^2$$

$$47 = 2^7 - 3^4$$

$$19 = 2^4 + 3^1$$

$$53 = ?$$

# Řešení Pohstova problému

M. Pohst (TU Berlin) :

Je možné zapsat libovolné prvočíslo  $p$  ve tvaru  $p = 2^u \pm 3^v$ ,  
 $u, v \in \mathbb{N}_0$ ?

**NE!**

$$2 = 2^0 + 3^0$$

$$23 = 2^5 - 3^2$$

$$3 = 2^1 + 3^0$$

$$29 = 2^1 + 3^3$$

$$5 = 2^1 + 3^1$$

$$31 = 2^2 + 3^3$$

$$7 = 2^2 + 3^1$$

$$37 = 2^6 - 3^3$$

$$11 = 2^1 + 3^2$$

$$41 = 2^5 + 3^2$$

$$13 = 2^2 + 3^2$$

$$43 = 2^4 + 3^3$$

$$17 = 2^3 + 3^2$$

$$47 = 2^7 - 3^4$$

$$19 = 2^4 + 3^1$$

$$53 = ?$$

Nejmenší prvočíslo, které nelze takto zapsat je 53.

**Děkuji za pozornost.**