Metoda nejmenších čtverců

Petr Vodstrčil

petr.vodstrcil@vsb.cz

VŠB TECHNICKÁ UNIVERZITA OSTRAVA | FAKULTA ELEKTROTECHNIKY A INFORMATIKY | KATEDRA APLIKOVANÉ MATEMATIKY

Ostrava, 22.1. 2025

(ŠKOMAM 2025)

Minimalizace kvadratické funkce

Příklad (Kvadratická funkce jedné proměnné)

Pro jaké $a \in \mathbb{R}$ je výraz

$$2a^2 - 6a + 1$$

minimální?

Minimalizace kvadratické funkce

Příklad (Kvadratická funkce jedné proměnné)

Pro jaké $a \in \mathbb{R}$ je výraz

$$2a^2 - 6a + 1$$

minimální? $\left[a = \frac{3}{2}\right]$

Minimalizace kvadratické funkce

Příklad (Kvadratická funkce jedné proměnné)

Pro jaké $a \in \mathbb{R}$ *je výraz*

$$2a^2 - 6a + 1$$

minimální? $\left[a = \frac{3}{2}\right]$

Příklad (Kvadratická funkce dvou proměnných)

Pro kterou dvojici $(a, b) \in \mathbb{R}^2$ *je výraz*

$$2a^2 + 21b^2 + 12ab - 20a - 72b + 11$$

minimální?

Minimalizace kvadratické funkce

Příklad (Kvadratická funkce jedné proměnné)

Pro jaké $a \in \mathbb{R}$ *je výraz*

$$2a^2 - 6a + 1$$

minimální? $\left[a = \frac{3}{2}\right]$

Příklad (Kvadratická funkce dvou proměnných)

Pro kterou dvojici $(a, b) \in \mathbb{R}^2$ *je výraz*

$$2a^2 + 21b^2 + 12ab - 20a - 72b + 11$$

minimální? $[a = -1,\ b = 2]$

Minimalizace obecné kvadratické funkce jedné proměnné

Pozorování

Nechť α, β, γ jsou reálné parametry. Je-li navíc $\alpha > 0$, pak výraz

$$\alpha a^2 + \beta a + \gamma$$

nabývá svého minima pro $a = -\frac{\beta}{2\alpha}$.

Minimalizace obecné kvadratické funkce jedné proměnné

Pozorování

Nechť α, β, γ jsou reálné parametry. Je-li navíc $\alpha > 0$, pak výraz

$$\alpha a^2 + \beta a + \gamma$$

nabývá svého minima pro $a = -\frac{\beta}{2\alpha}$.

Zdůvodnění

Doplněním na čtverec obdržíme

$$\alpha a^2 + \beta a + \gamma = \alpha \left[a^2 + \frac{\beta}{\alpha} a + \frac{\gamma}{\alpha} \right] = \alpha \left[\left(a + \frac{\beta}{2\alpha} \right)^2 - \frac{\beta^2}{4\alpha^2} + \frac{\gamma}{\alpha} \right] =$$

$$= \alpha \left(a + \frac{\beta}{2\alpha} \right)^2 - \frac{\beta^2 - 4\alpha\gamma}{4\alpha},$$

odkud plyne požadované tvrzení.

Metoda nejmenších čtverců

Uvažujme body $B_1 = [x_1, y_1], B_2 = [x_2, y_2], \ldots, B_n = [x_n, y_n]$ v rovině. Těmito body budeme chtít proložit tzv. regresní přímku. To je přímka, která co nejlépe „kopíruje“ zadané body.

Metoda nejmenších čtverců

Uvažujme body $B_1 = [x_1, y_1], B_2 = [x_2, y_2], \ldots, B_n = [x_n, y_n]$ v rovině. Těmito body budeme chtít proložit tzv. regresní přímku. To je přímka, která co nejlépe „kopíruje“ zadané body.

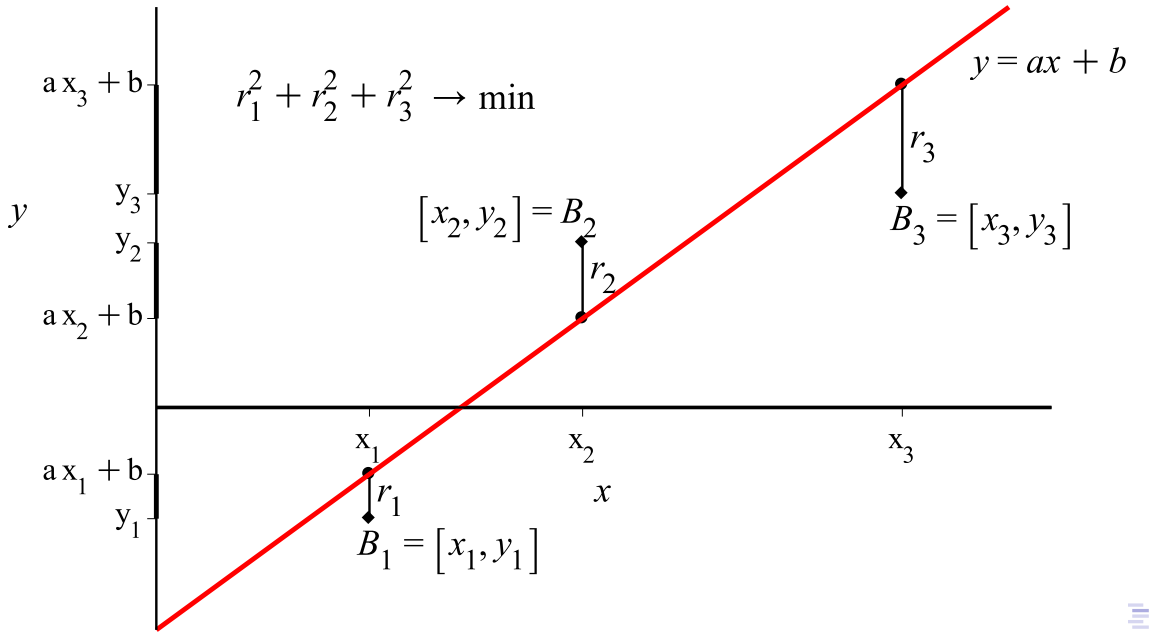
Rovnice takovéto přímky je $y = ax + b$, přičemž koeficienty $a, b \in \mathbb{R}$ volíme tak, aby výraz $\sum_{i=1}^{n} \left(ax_i + b - y_i\right)^2$ byl minimální (metoda nejmenších čtverců).

Metoda nejmenších čtverců

Uvažujme body $B_1 = [x_1, y_1], B_2 = [x_2, y_2], \ldots, B_n = [x_n, y_n]$ v rovině. Těmito body budeme chtít proložit tzv. regresní přímku. To je přímka, která co nejlépe „kopíruje“ zadané body.

Rovnice takovéto přímky je $y = ax + b$, přičemž koeficienty $a, b \in \mathbb{R}$ volíme tak, aby výraz $\sum_{i=1}^{n} \left(ax_i + b - y_i\right)^2$ byl minimální (metoda nejmenších čtverců).

Pro $n = 3$ je situace znázorněna na následujícím obrázku.



Poznámka

Danými body $B_1 = [x_1, y_1], B_2 = [x_2, y_2], \ldots, B_n = [x_n, y_n]$ nemusíme vždy prokládat jenom přímku $y = ax + b$. Např. je možné těmito body proložit přímku $y = ax$ (procházející počátkem), parabolu nebo jinou polynomickou funkci, exponenciálu, logaritmickou funkci, apod.

Poznámka

Danými body $B_1 = [x_1, y_1], B_2 = [x_2, y_2], \ldots, B_n = [x_n, y_n]$ nemusíme vždy prokládat jenom přímku $y = ax + b$. Např. je možné těmito body proložit přímku $y = ax$ (procházející počátkem), parabolu nebo jinou polynomickou funkci, exponenciálu, logaritmickou funkci, apod.

- V případě, že danými body chceme proložit přímku $y = ax$, musíme koeficient a zvolit tak, aby byl výraz $\sum_{i=1}^{n} (ax_i - y_i)^2$ minimální.

Poznámka

Danými body $B_1 = [x_1, y_1], B_2 = [x_2, y_2], \ldots, B_n = [x_n, y_n]$ nemusíme vždy prokládat jenom přímku $y = ax + b$. Např. je možné těmito body proložit přímku $y = ax$ (procházející počátkem), parabolu nebo jinou polynomickou funkci, exponenciálu, logaritmickou funkci, apod.

- V případě, že danými body chceme proložit přímku $y = ax$, musíme koeficient a zvolit tak, aby byl výraz $\sum_{i=1}^{n}(ax_i - y_i)^2$ minimální.
- Chceme-li našimi body proložit parabolu $y = ax^2 + bx + c$, zvolíme koeficienty a, b, c tak, aby výraz $\sum_{i=1}^{n}(ax_i^2 + bx_i + c - y_i)^2$ byl minimální.

Poznámka

Danými body $B_1 = [x_1, y_1], B_2 = [x_2, y_2], \ldots, B_n = [x_n, y_n]$ nemusíme vždy prokládat jenom přímku $y = ax + b$. Např. je možné těmito body proložit přímku $y = ax$ (procházející počátkem), parabolu nebo jinou polynomickou funkci, exponenciálu, logaritmickou funkci, apod.

- V případě, že danými body chceme proložit přímku $y = ax$, musíme koeficient a zvolit tak, aby byl výraz $\sum_{i=1}^{n}(ax_i - y_i)^2$ minimální.
- Chceme-li našimi body proložit parabolu $y = ax^2 + bx + c$, zvolíme koeficienty a, b, c tak, aby výraz $\sum_{i=1}^{n}(ax_i^2 + bx_i + c - y_i)^2$ byl minimální.

Za chvíli si ukážeme, jak danými body proložit přímku a parabolu.
V případě, že bychom chtěli uvažovat polynomy větších stupňů, postupovali bychom velmi podobně.

Příklad

Jsou dány body $B_1 = [1, 2]$, $B_2 = [2, 4]$, $B_3 = [4, 5]$. *Najděte regresní přímku procházející počátkem.*

Příklad

Jsou dány body $B_1 = [1, 2]$, $B_2 = [2, 4]$, $B_3 = [4, 5]$. Najděte regresní přímku procházející počátkem.

Řešení.

Přímka procházející počátkem má rovnici $y = ax$. Podle předchozího hledáme koeficient $a \in \mathbb{R}$ takový, aby výraz

$$\sum_{i=1}^{3} (ax_i - y_i)^2 = (a-2)^2 + (2a-4)^2 + (4a-5)^2 = 21a^2 - 60a + 45$$

byl minimální.

Příklad

Jsou dány body $B_1 = [1, 2]$, $B_2 = [2, 4]$, $B_3 = [4, 5]$. *Najděte regresní přímku procházející počátkem.*

Řešení.

Přímka procházející počátkem má rovnici $y = ax$. Podle předchozího hledáme koeficient $a \in \mathbb{R}$ takový, aby výraz

$$\sum_{i=1}^{3} (ax_i - y_i)^2 = (a-2)^2 + (2a-4)^2 + (4a-5)^2 = 21a^2 - 60a + 45$$

byl minimální. Jedná se o kvadratický výraz, který můžeme upravit na čtverec, tj.

$$21a^2 - 60a + 45 = 21\left(a^2 - \frac{20}{7}a + \frac{15}{7}\right) =$$

$$= 21\left[\left(a - \frac{10}{7}\right)^2 - \left(\frac{10}{7}\right)^2 + \frac{15}{7}\right] = 21\left(a - \frac{10}{7}\right)^2 + \frac{15}{7}.$$

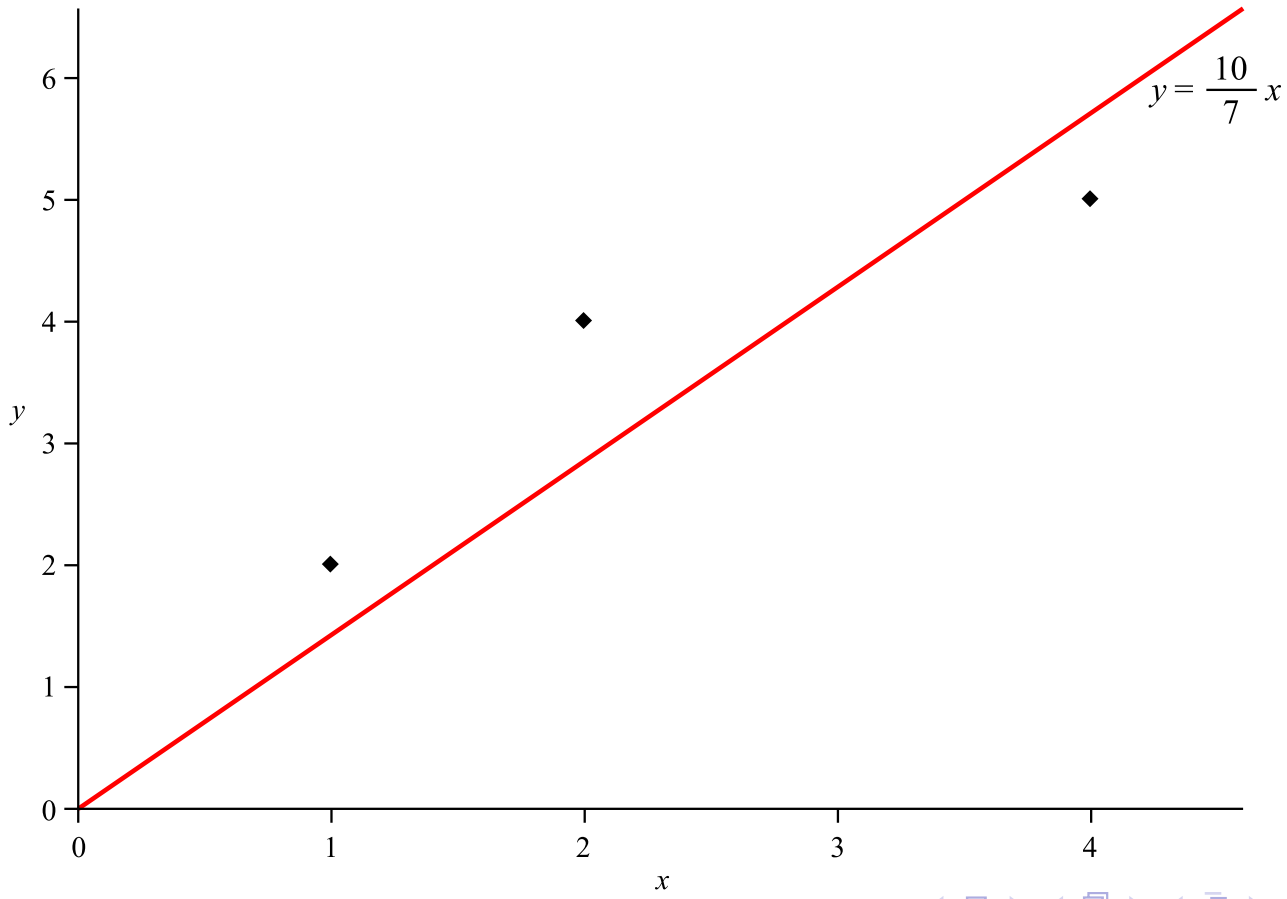
Řešení.

Vidíme tedy, že výraz je minimální pro $a = \frac{10}{7}$ a hledaná regresní přímka má rovnici $y = \frac{10}{7}x$. □

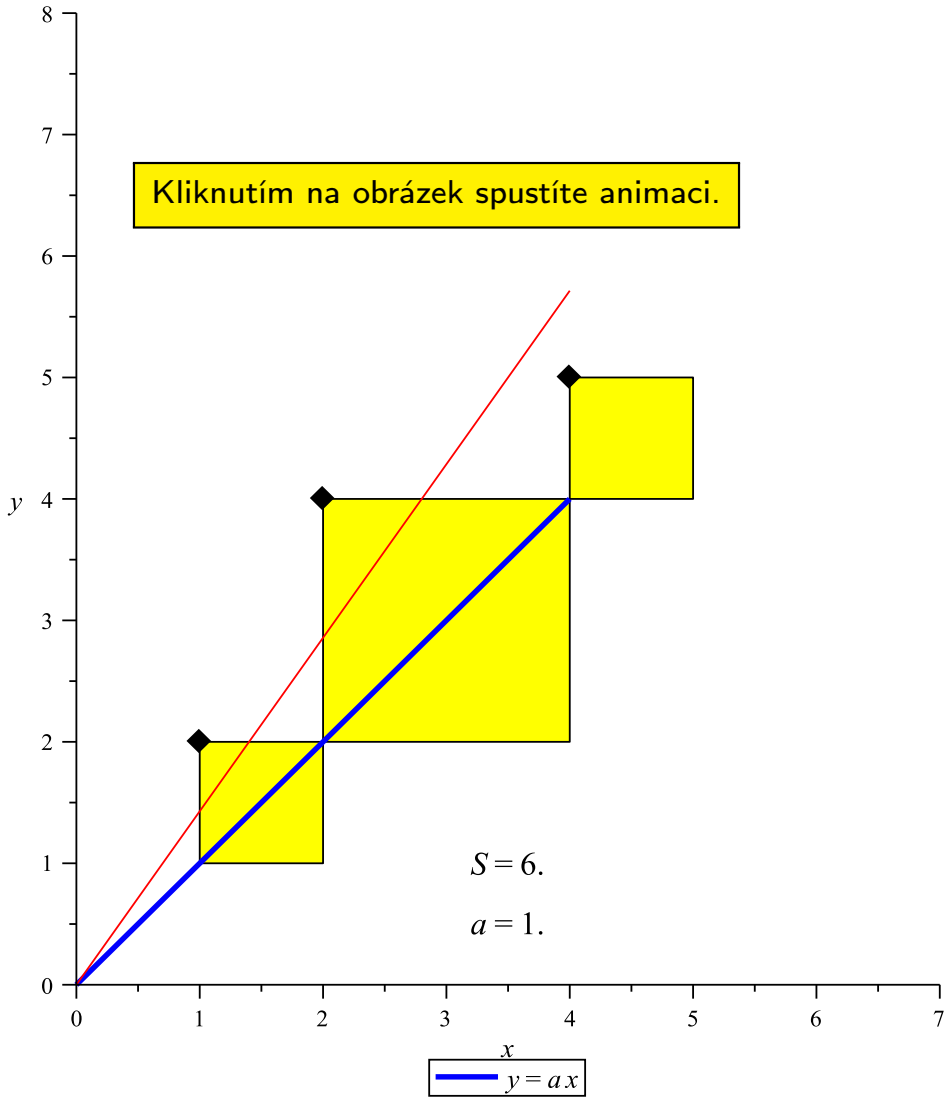
Řešení.

Vidíme tedy, že výraz je minimální pro $a = \frac{10}{7}$ a hledaná regresní přímka má rovnici $y = \frac{10}{7}x$. □

Situace je znázorněna na následujícím obrázku.

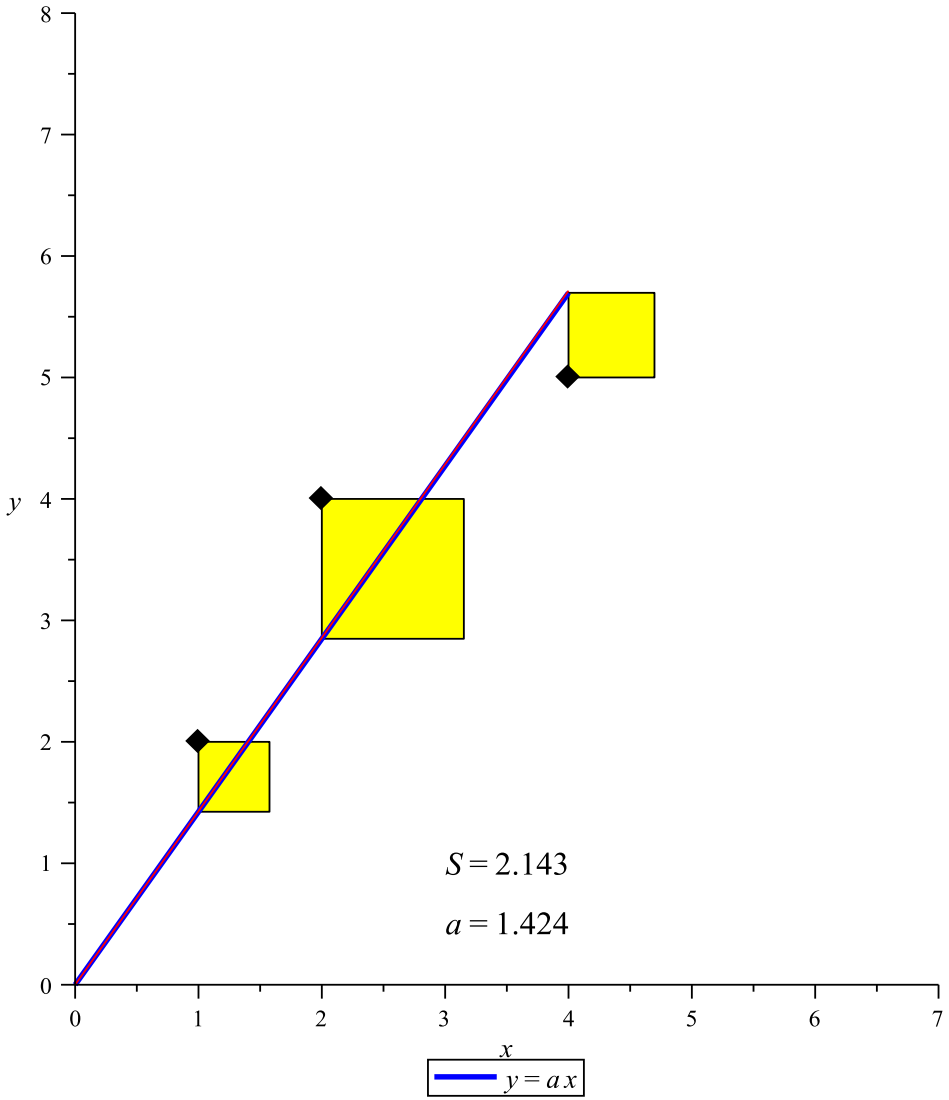


Animace



V případě problémů zkuste animaci spustit kliknutím na tento text.

Animace



Poznámka (Zobecnění pro n bodů)

Je-li dáno n bodů $B_1 = [x_1, y_1], B_2 = [x_2, y_2], \ldots, B_n = [x_n, y_n]$, pak regresní přímka procházející počátkem má rovnici

$$y = ax,$$

kde

$$a = \frac{\sum_{i=1}^{n} x_i y_i}{\sum_{i=1}^{n} x_i^2}.$$

Poznámka (Zobecnění pro n bodů)

Je-li dáno n bodů $B_1 = [x_1, y_1], B_2 = [x_2, y_2], \ldots, B_n = [x_n, y_n]$, pak regresní přímka procházející počátkem má rovnici

$$y = ax,$$

kde

$$a = \frac{\sum_{i=1}^{n} x_i y_i}{\sum_{i=1}^{n} x_i^2}.$$

Výraz $$\sum_{i=1}^{n} (ax_i - y_i)^2 = a^2 \sum_{i=1}^{n} x_i^2 - 2a \sum_{i=1}^{n} x_i y_i + \sum_{i=1}^{n} y_i^2$$

je totiž minimální právě pro $a = \frac{\sum_{i=1}^{n} x_i y_i}{\sum_{i=1}^{n} x_i^2}$.

Příklad

Jsou dány body $B_1 = [1, 2]$, $B_2 = [2, 4]$, $B_3 = [4, 5]$ (*stejné jako v předchozím příkladu*). *Najděte regresní přímku* $y = ax + b$.

Příklad

Jsou dány body $B_1 = [1, 2]$, $B_2 = [2, 4]$, $B_3 = [4, 5]$ (*stejné jako v předchozím příkladu*). *Najděte regresní přímku* $y = ax + b$.

Řešení.

Rovnice hledané přímky je $y = ax + b$. Koeficienty $a, b \in \mathbb{R}$ přitom musíme zvolit tak, aby byl výraz

$$\sum_{i=1}^{3} \left(ax_i + b - y_i\right)^2 = (a + b - 2)^2 + (2a + b - 4)^2 + (4a + b - 5)^2$$

minimální.

Příklad

Jsou dány body $B_1 = [1, 2]$, $B_2 = [2, 4]$, $B_3 = [4, 5]$ (*stejné jako v předchozím příkladu*). *Najděte regresní přímku* $y = ax + b$.

Řešení.

Rovnice hledané přímky je $y = ax + b$. Koeficienty $a, b \in \mathbb{R}$ přitom musíme zvolit tak, aby byl výraz

$$\sum_{i=1}^{3} \left(ax_i + b - y_i\right)^2 = (a + b - 2)^2 + (2a + b - 4)^2 + (4a + b - 5)^2 =$$

$$= 21a^2 + 14ab + 3b^2 - 60a - 22b + 45$$

minimální.

Příklad

Jsou dány body $B_1 = [1, 2]$, $B_2 = [2, 4]$, $B_3 = [4, 5]$ (*stejné jako v předchozím příkladu*). *Najděte regresní přímku* $y = ax + b$.

Řešení.

Rovnice hledané přímky je $y = ax + b$. Koeficienty $a, b \in \mathbb{R}$ přitom musíme zvolit tak, aby byl výraz

$$\sum_{i=1}^{3} (ax_i + b - y_i)^2 = (a + b - 2)^2 + (2a + b - 4)^2 + (4a + b - 5)^2 =$$

$$= 21a^2 + 14ab + 3b^2 - 60a - 22b + 45 =$$

$$= 3\left(b + \frac{7}{3}a - \frac{11}{3}\right)^2 + \frac{14}{3}\left(a - \frac{13}{14}\right)^2 + \frac{9}{14}$$

minimální.

Příklad

Jsou dány body $B_1 = [1, 2]$, $B_2 = [2, 4]$, $B_3 = [4, 5]$ (*stejné jako v předchozím příkladu*). *Najděte regresní přímku* $y = ax + b$.

Řešení.

Rovnice hledané přímky je $y = ax + b$. Koeficienty $a, b \in \mathbb{R}$ přitom musíme zvolit tak, aby byl výraz

$$\sum_{i=1}^{3} (ax_i + b - y_i)^2 = (a + b - 2)^2 + (2a + b - 4)^2 + (4a + b - 5)^2 =$$

$$= 21a^2 + 14ab + 3b^2 - 60a - 22b + 45 =$$

$$= 3\left(b + \frac{7}{3}a - \frac{11}{3}\right)^2 + \frac{14}{3}\left(a - \frac{13}{14}\right)^2 + \frac{9}{14}$$

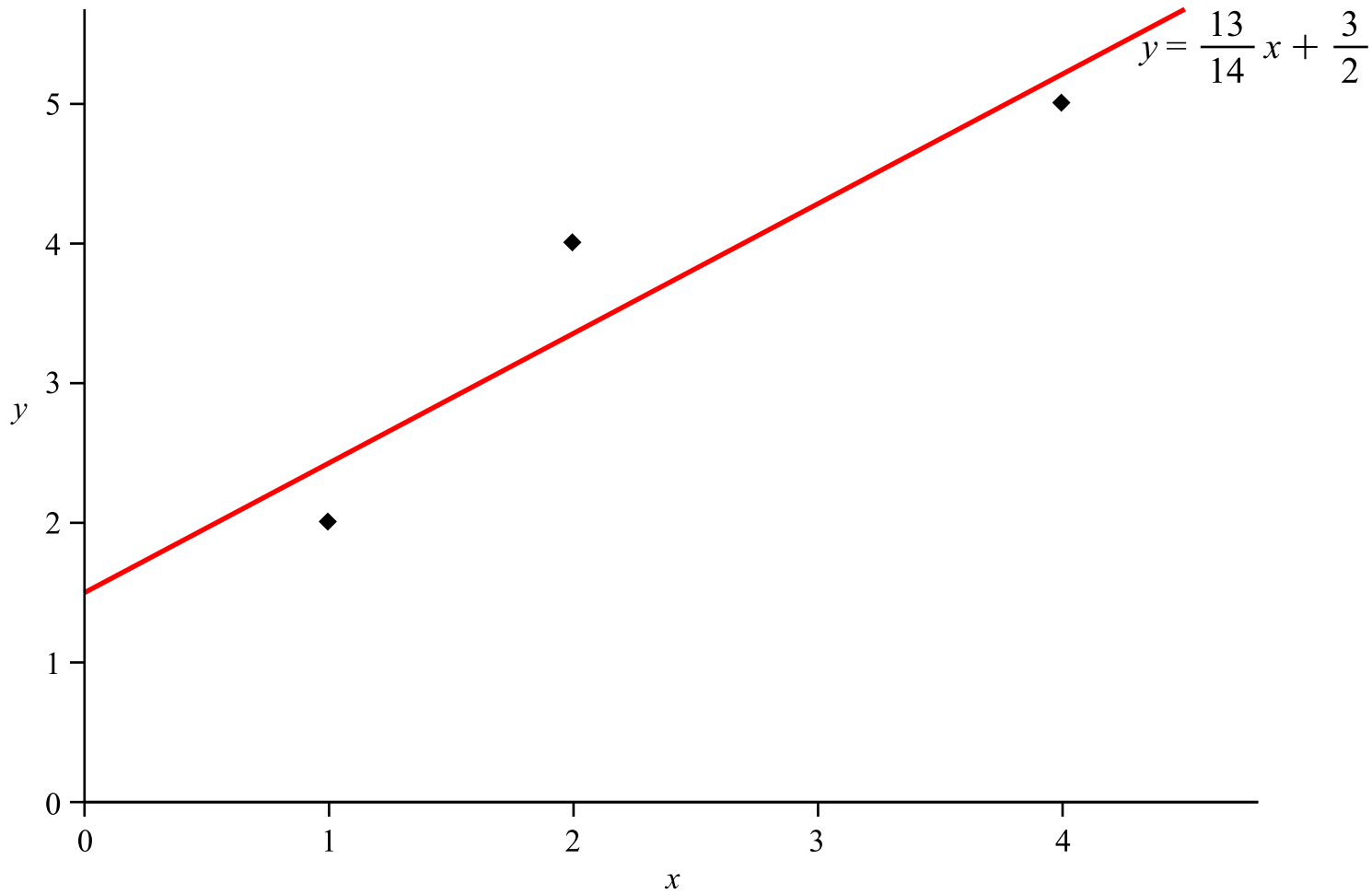
minimální.

To nastane v případě, že $a = \frac{13}{14}$ a $b = \frac{3}{2}$.

Hledaná regresní přímka má rovnici $y = \frac{13}{14}x + \frac{3}{2}$.

Hledaná regresní přímka má rovnici $y = \frac{13}{14}x + \frac{3}{2}$.

Celou situaci opět vystihuje obrázek.



Poznámka (Zobecnění pro n bodů)

Je-li dáno n bodů $B_1 = [x_1, y_1], B_2 = [x_2, y_2], \ldots, B_n = [x_n, y_n]$, pak regresní přímka má rovnici

$$y = ax + b,$$

kde

$$a = \frac{n\left(\sum_{i=1}^{n} x_i y_i\right) - \left(\sum_{i=1}^{n} x_i\right)\left(\sum_{i=1}^{n} y_i\right)}{n\left(\sum_{i=1}^{n} x_i^2\right) - \left(\sum_{i=1}^{n} x_i\right)^2}$$

a

$$b = \frac{\left(\sum_{i=1}^{n} y_i\right)\left(\sum_{i=1}^{n} x_i^2\right) - \left(\sum_{i=1}^{n} x_i\right)\left(\sum_{i=1}^{n} x_i y_i\right)}{n\left(\sum_{i=1}^{n} x_i^2\right) - \left(\sum_{i=1}^{n} x_i\right)^2}.$$

Příklad

Jsou dány body $B_1 = [0, 0]$, $B_2 = [1, 1]$, $B_3 = [2, 3]$, $B_4 = [3, 8]$. *Proložte těmito body parabolu* $y = ax^2$.

Příklad

Jsou dány body $B_1 = [0, 0]$, $B_2 = [1, 1]$, $B_3 = [2, 3]$, $B_4 = [3, 8]$. *Proložte těmito body parabolu* $y = ax^2$.

Řešení.

Rovnice hledané paraboly je $y = ax^2$. Koeficient $a \in \mathbb{R}$ přitom musíme zvolit tak, aby byl výraz

$$\sum_{i=1}^{4} \left(ax_i^2 - y_i\right)^2 = (0-0)^2 + (a-1)^2 + (4a-3)^2 + (9a-8)^2$$

minimální.

Příklad

Jsou dány body $B_1 = [0, 0]$, $B_2 = [1, 1]$, $B_3 = [2, 3]$, $B_4 = [3, 8]$. *Proložte těmito body parabolu* $y = ax^2$.

Řešení.

Rovnice hledané paraboly je $y = ax^2$. Koeficient $a \in \mathbb{R}$ přitom musíme zvolit tak, aby byl výraz

$$\sum_{i=1}^{4} \left(ax_i^2 - y_i\right)^2 = (0-0)^2 + (a-1)^2 + (4a-3)^2 + (9a-8)^2 =$$
$$= (a^2 - 2a + 1) + (16a^2 - 24a + 9) + (81a^2 - 144a + 64)$$

minimální.

Příklad

Jsou dány body $B_1 = [0, 0]$, $B_2 = [1, 1]$, $B_3 = [2, 3]$, $B_4 = [3, 8]$. *Proložte těmito body parabolu* $y = ax^2$.

Řešení.

Rovnice hledané paraboly je $y = ax^2$. Koeficient $a \in \mathbb{R}$ přitom musíme zvolit tak, aby byl výraz

$$\sum_{i=1}^{4} \left(ax_i^2 - y_i\right)^2 = (0-0)^2 + (a-1)^2 + (4a-3)^2 + (9a-8)^2 =$$

$$= (a^2 - 2a + 1) + (16a^2 - 24a + 9) + (81a^2 - 144a + 64) =$$

$$= 98a^2 - 170a + 74$$

minimální.

Příklad

Jsou dány body $B_1 = [0, 0]$, $B_2 = [1, 1]$, $B_3 = [2, 3]$, $B_4 = [3, 8]$. *Proložte těmito body parabolu* $y = ax^2$.

Řešení.

Rovnice hledané paraboly je $y = ax^2$. Koeficient $a \in \mathbb{R}$ přitom musíme zvolit tak, aby byl výraz

$$\sum_{i=1}^{4} \left(ax_i^2 - y_i\right)^2 = (0-0)^2 + (a-1)^2 + (4a-3)^2 + (9a-8)^2 =$$

$$= (a^2 - 2a + 1) + (16a^2 - 24a + 9) + (81a^2 - 144a + 64) =$$

$$= 98a^2 - 170a + 74 = 98\left(a^2 - \frac{170}{98}a + \frac{74}{98}\right)$$

minimální.

Příklad

Jsou dány body $B_1 = [0,0]$, $B_2 = [1,1]$, $B_3 = [2,3]$, $B_4 = [3,8]$. *Proložte těmito body parabolu* $y = ax^2$.

Řešení.

Rovnice hledané paraboly je $y = ax^2$. Koeficient $a \in \mathbb{R}$ přitom musíme zvolit tak, aby byl výraz

$$\sum_{i=1}^{4} \left(ax_i^2 - y_i\right)^2 = (0-0)^2 + (a-1)^2 + (4a-3)^2 + (9a-8)^2 =$$

$$= (a^2 - 2a + 1) + (16a^2 - 24a + 9) + (81a^2 - 144a + 64) =$$

$$= 98a^2 - 170a + 74 = 98\left(a^2 - \frac{170}{98}a + \frac{74}{98}\right) = 98\left(a - \frac{85}{98}\right)^2 + \frac{27}{98}$$

minimální.

Příklad

Jsou dány body $B_1 = [0, 0]$, $B_2 = [1, 1]$, $B_3 = [2, 3]$, $B_4 = [3, 8]$. *Proložte těmito body parabolu* $y = ax^2$.

Řešení.

Rovnice hledané paraboly je $y = ax^2$. Koeficient $a \in \mathbb{R}$ přitom musíme zvolit tak, aby byl výraz

$$\sum_{i=1}^{4} \left(ax_i^2 - y_i\right)^2 = (0-0)^2 + (a-1)^2 + (4a-3)^2 + (9a-8)^2 =$$

$$= (a^2 - 2a + 1) + (16a^2 - 24a + 9) + (81a^2 - 144a + 64) =$$

$$= 98a^2 - 170a + 74 = 98\left(a^2 - \frac{170}{98}a + \frac{74}{98}\right) = 98\left(a - \frac{85}{98}\right)^2 + \frac{27}{98}$$

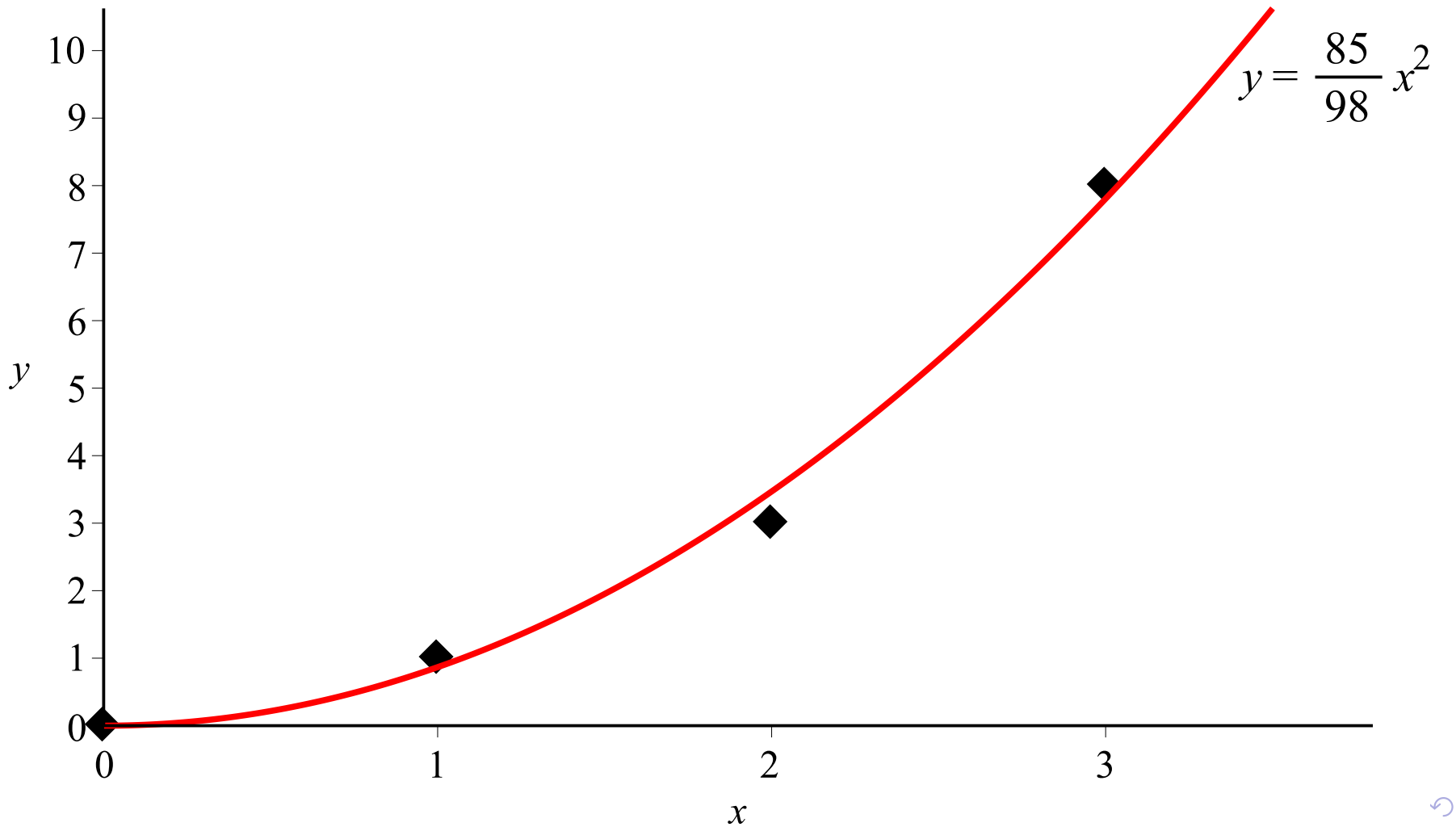
minimální.

To nastane v případě, že $a = \frac{85}{98}$.

Hledaná parabola má rovnici $y = \frac{85}{98}x^2$.

Hledaná parabola má rovnici $y = \frac{85}{98}x^2$.

Grafické znázornění:



Poznámka (Zobecnění pro n bodů)

Nechť je dáno n bodů $B_1 = [x_1, y_1], B_2 = [x_2, y_2], \ldots, B_n = [x_n, y_n]$.
Parabola $y = ax^2$ tyto body nejlépe „kopíruje“, platí-li

$$a = \frac{\sum_{i=1}^{n} x_i^2 y_i}{\sum_{i=1}^{n} x_i^4}.$$

Poznámka (Zobecnění pro n bodů)

Nechť je dáno n bodů $B_1 = [x_1, y_1], B_2 = [x_2, y_2], \ldots, B_n = [x_n, y_n]$.
Parabola $y = ax^2$ tyto body nejlépe „kopíruje“, platí-li

$$a = \frac{\sum_{i=1}^{n} x_i^2 y_i}{\sum_{i=1}^{n} x_i^4}.$$

Výraz $$\sum_{i=1}^{n} (ax_i^2 - y_i)^2 = a^2 \sum_{i=1}^{n} x_i^4 - 2a \sum_{i=1}^{n} x_i^2 y_i + \sum_{i=1}^{n} y_i^2$$

je totiž minimální právě pro $a = \frac{\sum_{i=1}^{n} x_i^2 y_i}{\sum_{i=1}^{n} x_i^4}$.

Příklad

Jsou dány body $B_1 = [0, 0]$, $B_2 = [1, 1]$, $B_3 = [2, 3]$, $B_4 = [3, 8]$. *Proložte těmito body parabolu* $y = ax^2 + bx + c$.

Příklad

Jsou dány body $B_1 = [0, 0]$, $B_2 = [1, 1]$, $B_3 = [2, 3]$, $B_4 = [3, 8]$. *Proložte těmito body parabolu* $y = ax^2 + bx + c$.

Řešení.

Rovnice hledané paraboly je $y = ax^2 + bx + c$. Koeficienty $a, b, c \in \mathbb{R}$ přitom musíme zvolit tak, aby byl výraz

$$\sum_{i=1}^{4} \left(ax_i^2 + bx_i + c - y_i\right)^2 =$$
$$= c^2 + (a + b + c - 1)^2 + (4a + 2b + c - 3)^2 + (9a + 3b + c - 8)^2$$

minimální.

Příklad

Jsou dány body $B_1 = [0, 0]$, $B_2 = [1, 1]$, $B_3 = [2, 3]$, $B_4 = [3, 8]$. *Proložte těmito body parabolu* $y = ax^2 + bx + c$.

Řešení.

Rovnice hledané paraboly je $y = ax^2 + bx + c$. Koeficienty $a, b, c \in \mathbb{R}$ přitom musíme zvolit tak, aby byl výraz

$$\sum_{i=1}^{4} \left(ax_i^2 + bx_i + c - y_i\right)^2 =$$

$$= c^2 + (a + b + c - 1)^2 + (4a + 2b + c - 3)^2 + (9a + 3b + c - 8)^2 =$$

$$= 98a^2 + 72ab + 28ac + 14b^2 + 12bc + 4c^2 - 170a - 62b - 24c + 74$$

minimální.

Příklad

Jsou dány body $B_1 = [0,0]$, $B_2 = [1,1]$, $B_3 = [2,3]$, $B_4 = [3,8]$. *Proložte těmito body parabolu* $y = ax^2 + bx + c$.

Řešení.

Rovnice hledané paraboly je $y = ax^2 + bx + c$. Koeficienty $a, b, c \in \mathbb{R}$ přitom musíme zvolit tak, aby byl výraz

$$\sum_{i=1}^{4} \left(ax_i^2 + bx_i + c - y_i\right)^2 =$$

$$= c^2 + (a + b + c - 1)^2 + (4a + 2b + c - 3)^2 + (9a + 3b + c - 8)^2 =$$

$$= 98a^2 + 72ab + 28ac + 14b^2 + 12bc + 4c^2 - 170a - 62b - 24c + 74 =$$

$$4\left(c + \tfrac{3}{2}b + \tfrac{7}{2}a - 3\right)^2 + 5\left(b + 3a - \tfrac{13}{5}\right)^2 + 4(a-1)^2 + \tfrac{1}{5}$$

minimální.

Příklad

Jsou dány body $B_1 = [0,0]$, $B_2 = [1,1]$, $B_3 = [2,3]$, $B_4 = [3,8]$. *Proložte těmito body parabolu* $y = ax^2 + bx + c$.

Řešení.

Rovnice hledané paraboly je $y = ax^2 + bx + c$. Koeficienty $a, b, c \in \mathbb{R}$ přitom musíme zvolit tak, aby byl výraz

$$\sum_{i=1}^{4} \left(ax_i^2 + bx_i + c - y_i\right)^2 =$$

$$= c^2 + (a + b + c - 1)^2 + (4a + 2b + c - 3)^2 + (9a + 3b + c - 8)^2 =$$

$$= 98a^2 + 72ab + 28ac + 14b^2 + 12bc + 4c^2 - 170a - 62b - 24c + 74 =$$

$$4\left(c + \tfrac{3}{2}b + \tfrac{7}{2}a - 3\right)^2 + 5\left(b + 3a - \tfrac{13}{5}\right)^2 + 4(a-1)^2 + \tfrac{1}{5}$$

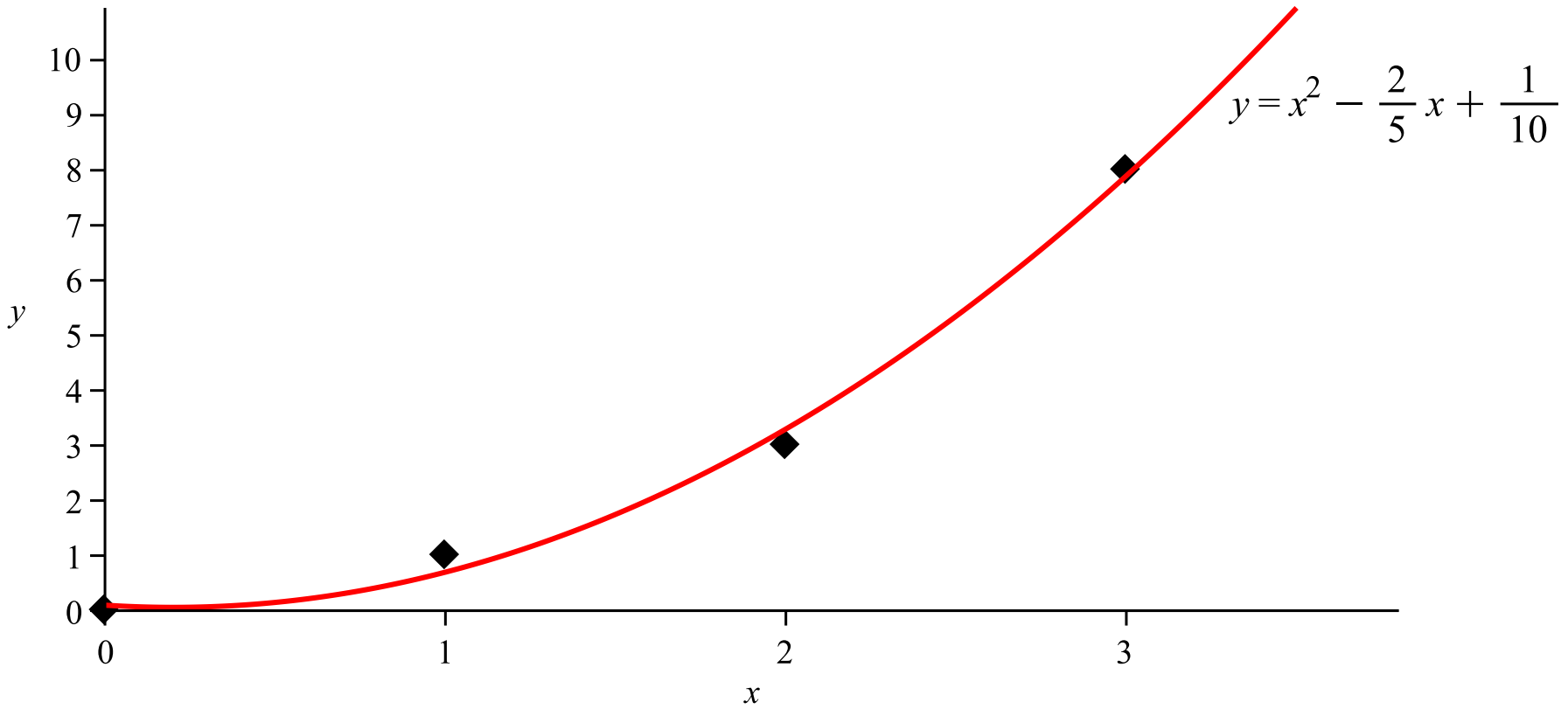
minimální.

To nastane v případě, že $a = 1$, $b = -\frac{2}{5}$ a $c = \frac{1}{10}$.

Hledaná parabola má rovnici $y = x^2 - \frac{2}{5}x + \frac{1}{10}$.

Hledaná parabola má rovnici $y = x^2 - \frac{2}{5}x + \frac{1}{10}$.

Grafické znázornění:



Prokládání exponenciály

Co dělat, když se data $[x_1, y_1]$, $[x_2, y_2]$, $\ldots$, $[x_n, y_n]$ chovají exponenciálně,

Prokládání exponenciály

Co dělat, když se data $[x_1, y_1]$, $[x_2, y_2]$, $\ldots$, $[x_n, y_n]$ chovají exponenciálně, tzn. přibližně kopírují graf funkce

$$y = \alpha e^{\beta x}$$

pro nějaká $\alpha, \beta \in \mathbb{R}$.

Prokládání exponenciály

Co dělat, když se data $[x_1, y_1]$, $[x_2, y_2]$, $\ldots$, $[x_n, y_n]$ chovají exponenciálně, tzn. přibližně kopírují graf funkce

$$y = \alpha e^{\beta x}$$

pro nějaká $\alpha, \beta \in \mathbb{R}$.

Pokud je $\alpha > 0$, pak podle pravidel pro počítání s logaritmy dostaneme

$$\ln y = \ln \alpha + \beta x,$$

Prokládání exponenciály

Co dělat, když se data $[x_1, y_1]$, $[x_2, y_2]$, $\ldots$, $[x_n, y_n]$ chovají exponenciálně, tzn. přibližně kopírují graf funkce

$$y = \alpha e^{\beta x}$$

pro nějaká $\alpha, \beta \in \mathbb{R}$.

Pokud je $\alpha > 0$, pak podle pravidel pro počítání s logaritmy dostaneme

$$\ln y = \ln \alpha + \beta x,$$

což znamená, že data

$$[x_1, \ln y_1], [x_2, \ln y_2], \ldots, [x_n, \ln y_n]$$

se budou chovat přibližně lineárně,

Prokládání exponenciály

Co dělat, když se data $[x_1, y_1]$, $[x_2, y_2]$, $\ldots$, $[x_n, y_n]$ chovají exponenciálně, tzn. přibližně kopírují graf funkce

$$y = \alpha e^{\beta x}$$

pro nějaká $\alpha, \beta \in \mathbb{R}$.

Pokud je $\alpha > 0$, pak podle pravidel pro počítání s logaritmy dostaneme

$$\ln y = \ln \alpha + \beta x,$$

což znamená, že data

$$[x_1, \ln y_1], [x_2, \ln y_2], \ldots, [x_n, \ln y_n]$$

se budou chovat přibližně lineárně,
a tedy na ně lze použít předchozí metody.

Příklad (důležitý pro šifrování)

Vynásobíme-li mezi sebou dvě různá n ciferná prvočísla, která vzápětí zapomeneme, a výsledek budeme chtít zpětně rozložit na prvočinitele, bude čas výpočtu na n záviset přibližně exponenciálně. Budeme předpokládat, že

$$t(n) \approx \alpha e^{\beta n},$$

kde α a β jsou kladné konstanty závislé na použitém hardwaru a softwaru.

Příklad (důležitý pro šifrování)

Vynásobíme-li mezi sebou dvě různá n ciferná prvočísla, která vzápětí zapomeneme, a výsledek budeme chtít zpětně rozložit na prvočinitele, bude čas výpočtu na n záviset přibližně exponenciálně. Budeme předpokládat, že

$$t(n) \approx \alpha e^{\beta n},$$

kde α a β jsou kladné konstanty závislé na použitém hardwaru a softwaru.

Provedeme pokus tak, že budeme rozkládat čísla, která vznikla součinem dvou různých (náhodně vygenerovaných) n ciferných prvočísel, kde $n \in \{25, 26, \ldots, 40\}$. Budeme přitom zaznamenávat časy jednotlivých rozkladů. Celý pokus zopakujeme $3\times$ a odpovídající časy zprůměrujeme.

Příklad (důležitý pro šifrování)

Vynásobíme-li mezi sebou dvě různá n ciferná prvočísla, která vzápětí zapomeneme, a výsledek budeme chtít zpětně rozložit na prvočinitele, bude čas výpočtu na n záviset přibližně exponenciálně. Budeme předpokládat, že

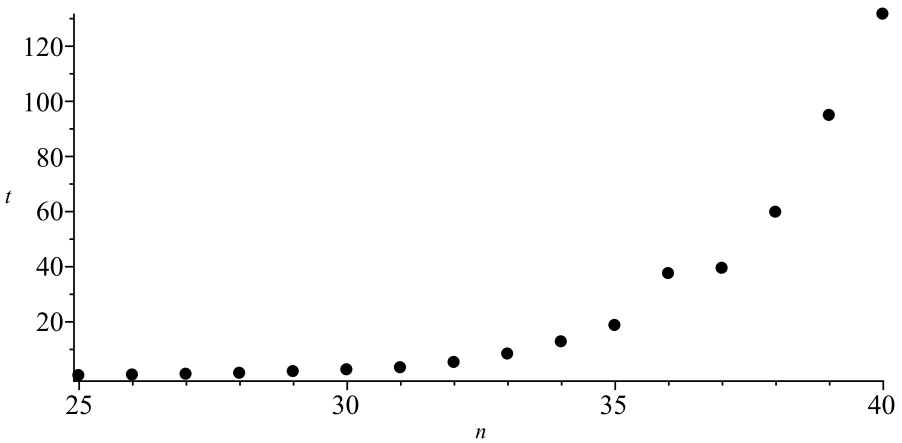
$$t(n) \approx \alpha e^{\beta n},$$

kde α a β jsou kladné konstanty závislé na použitém hardwaru a softwaru.

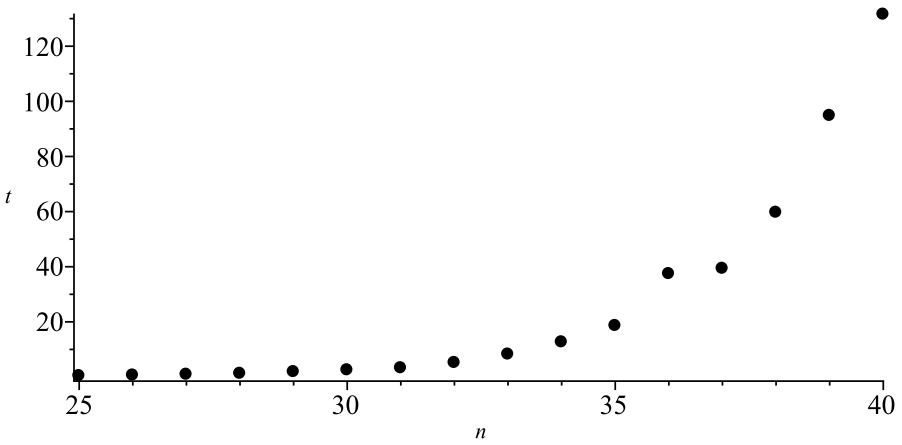
Provedeme pokus tak, že budeme rozkládat čísla, která vznikla součinem dvou různých (náhodně vygenerovaných) n ciferných prvočísel, kde $n \in \{25, 26, \ldots, 40\}$. Budeme přitom zaznamenávat časy jednotlivých rozkladů. Celý pokus zopakujeme $3\times$ a odpovídající časy zprůměrujeme.

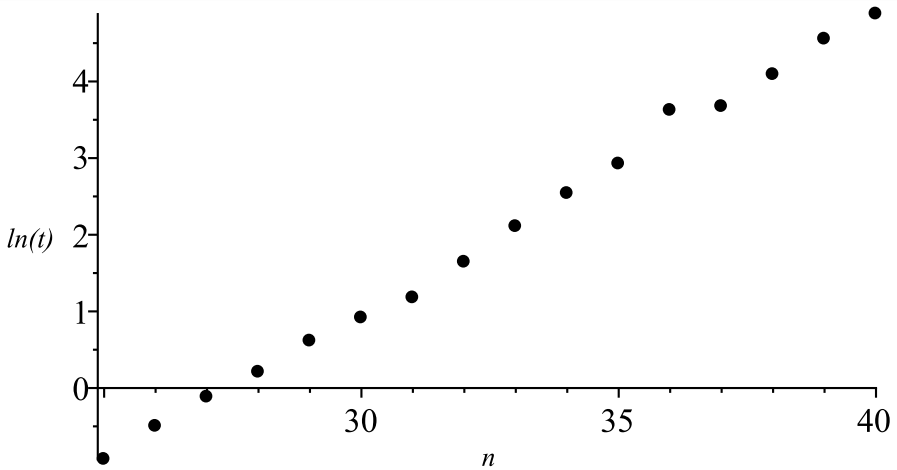
Cílem bude predikovat, jak dlouho by trval rozklad čísla, které vzniklo součinem například dvou 100 ciferných prvočísel.

Naměřené časy

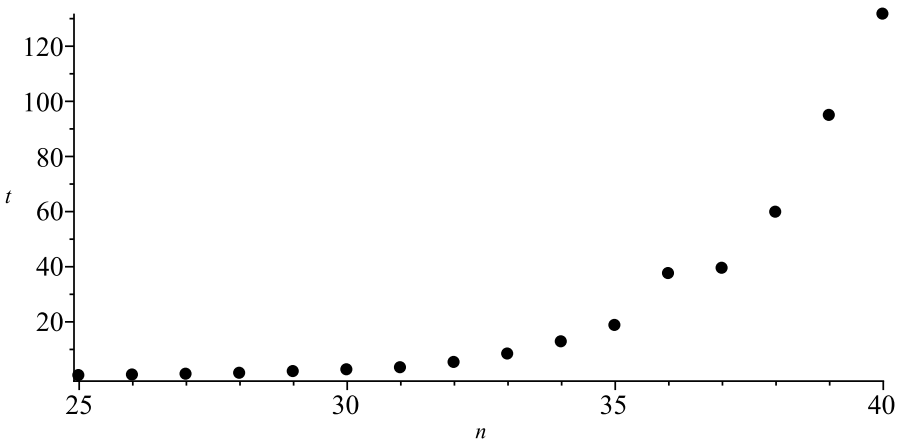


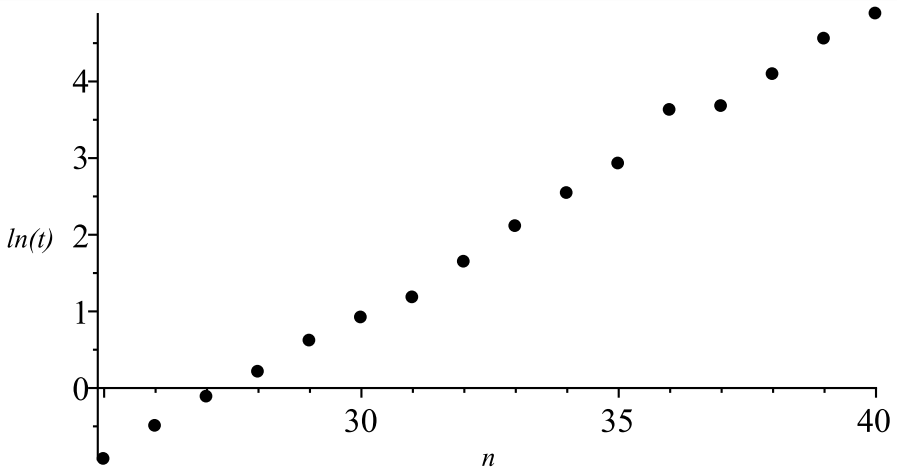
Naměřené časy

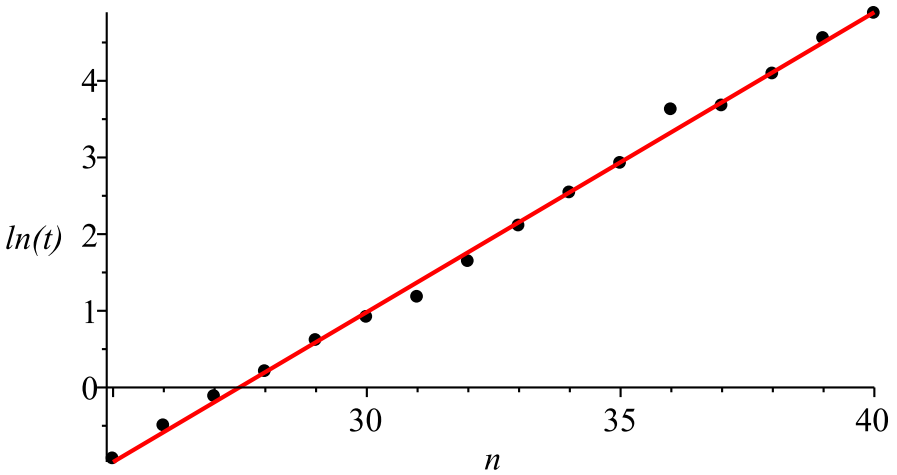




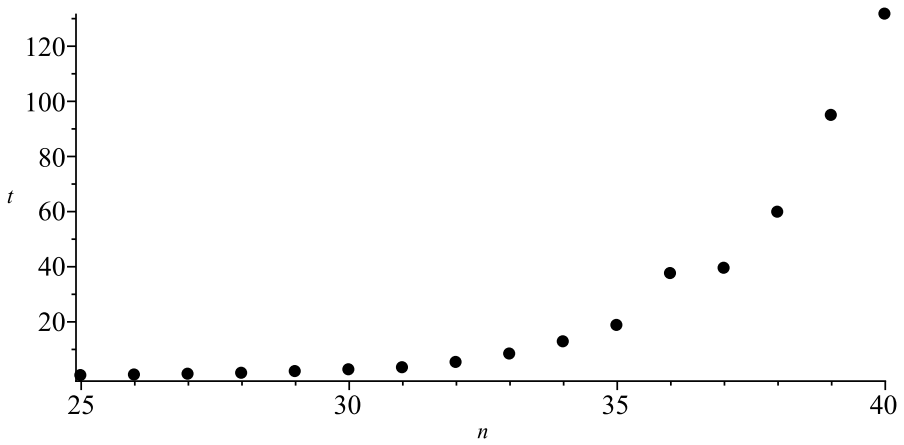
Naměřené časy

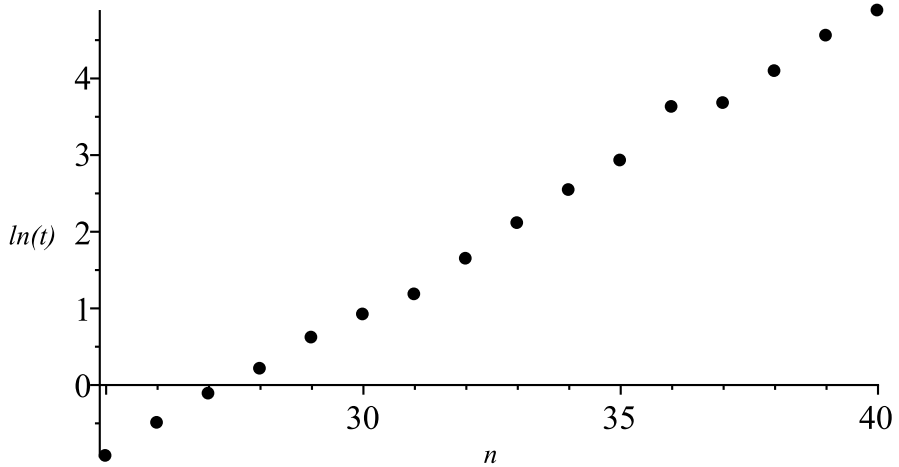


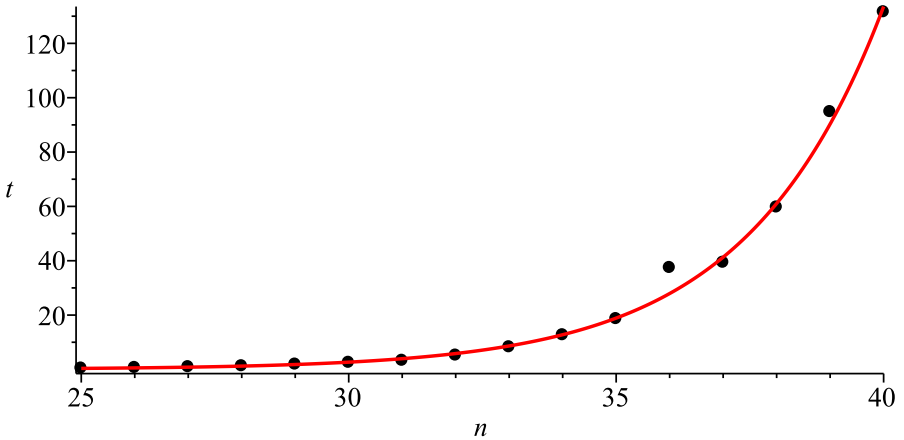


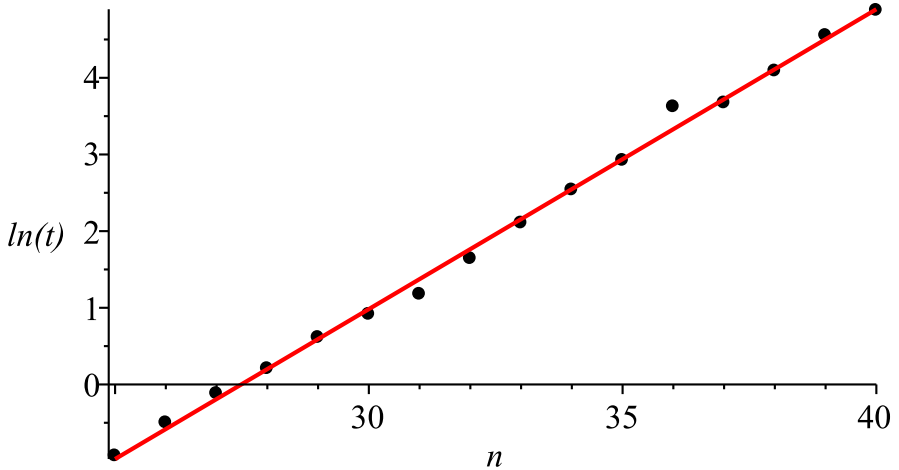


Naměřené časy

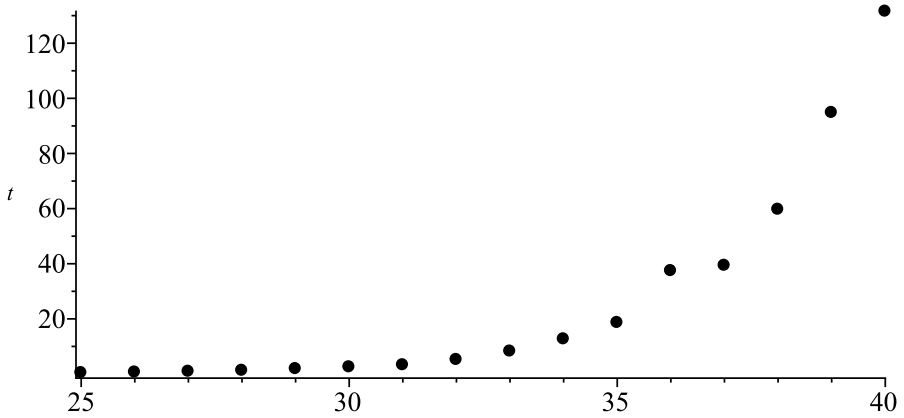


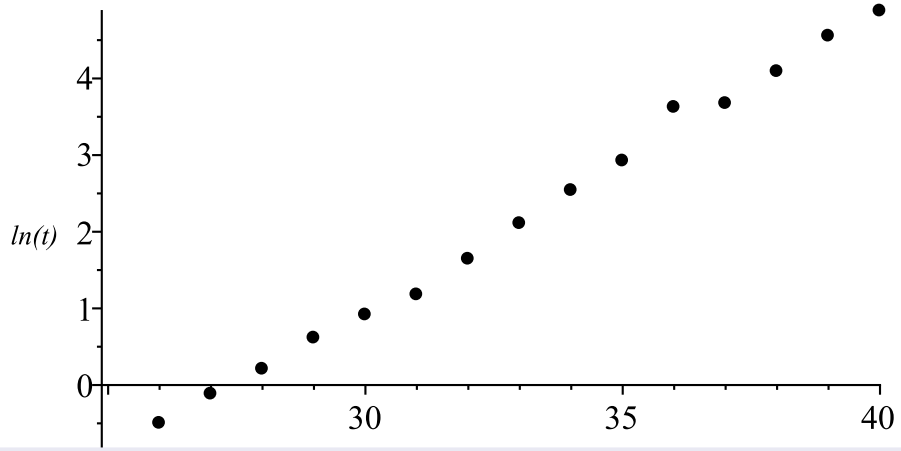




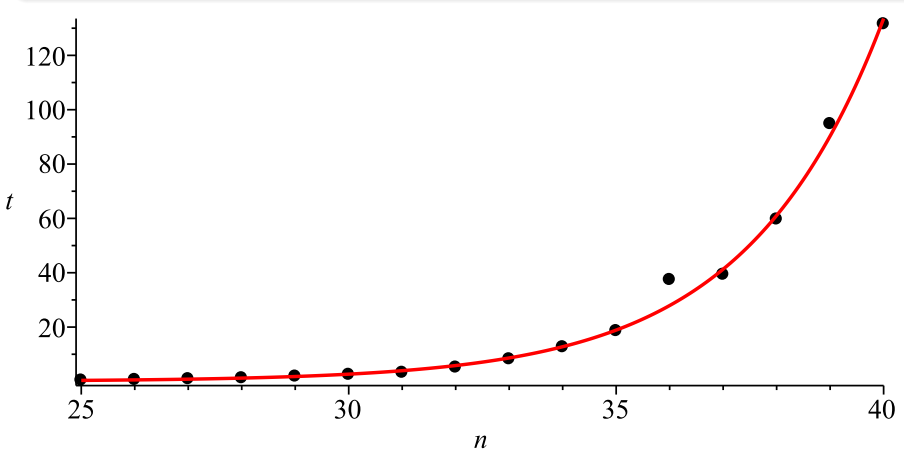


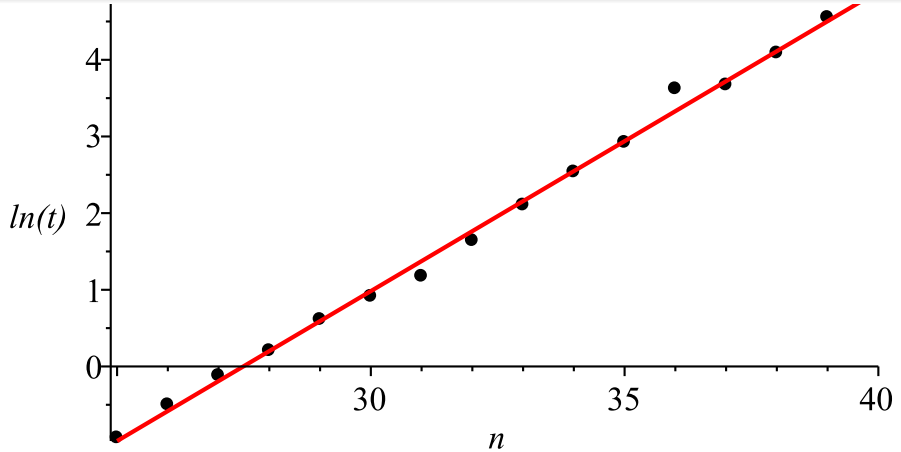
Naměřené časy



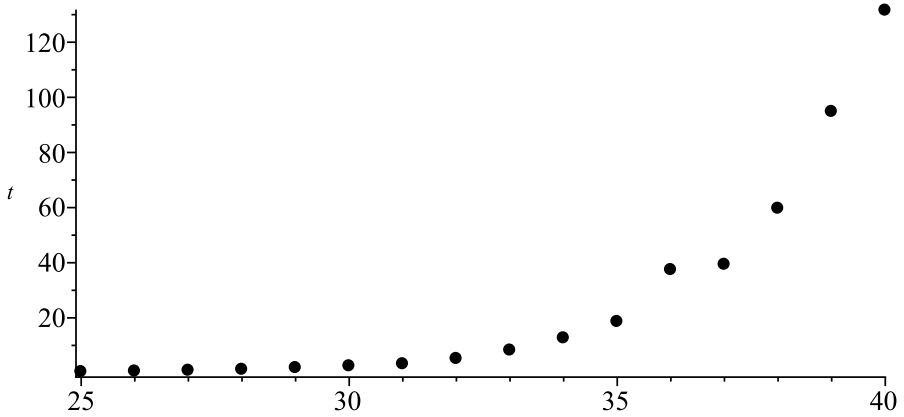


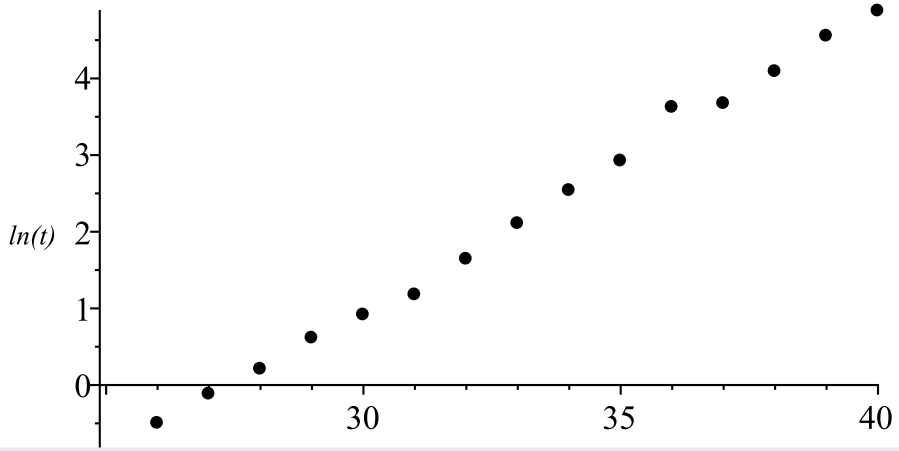
$t(n) \approx 0.000021408867798\, e^{0.391154069618199n}$



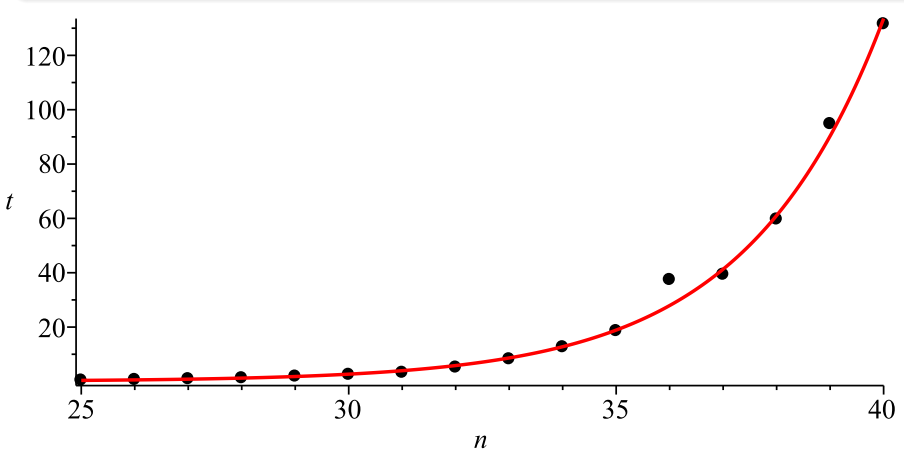


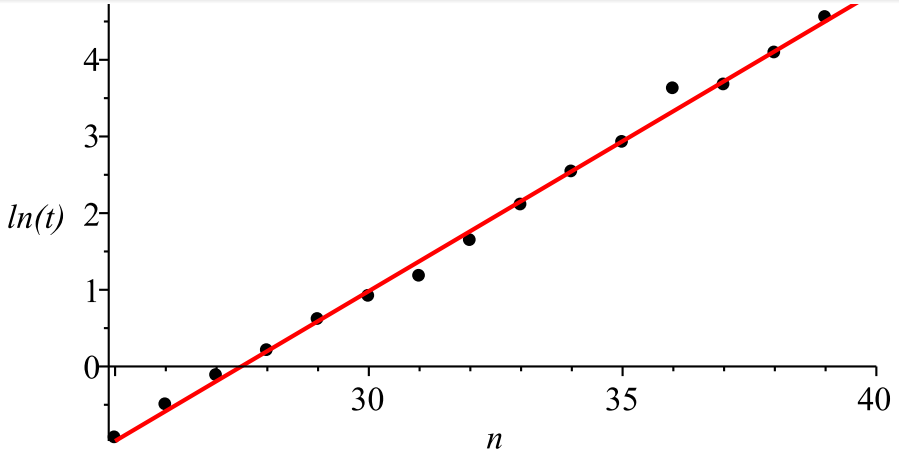
Naměřené časy





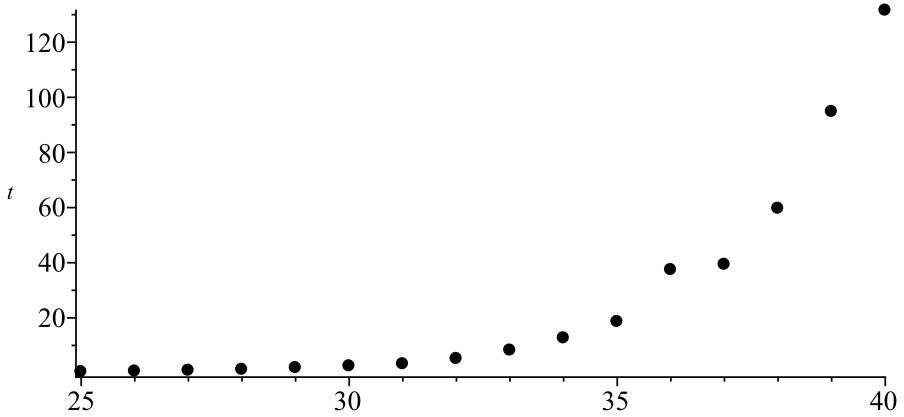
$t(n) \approx 0.000021408867798\, e^{0.391154069618199n}$

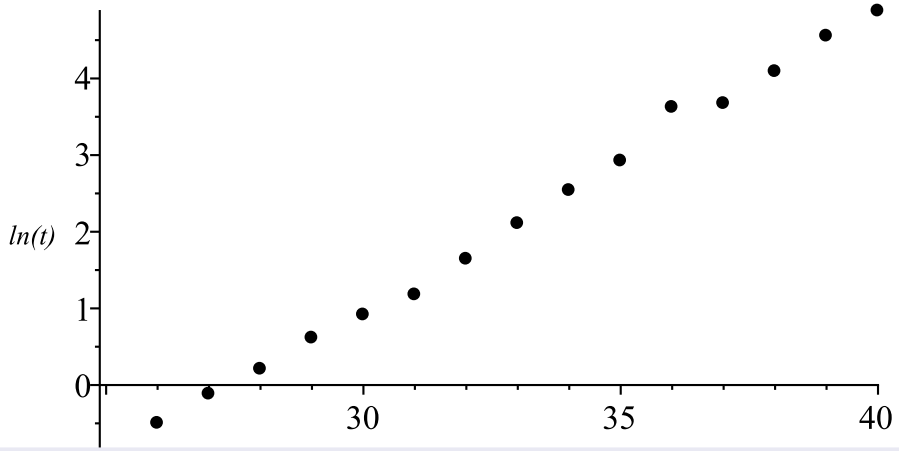




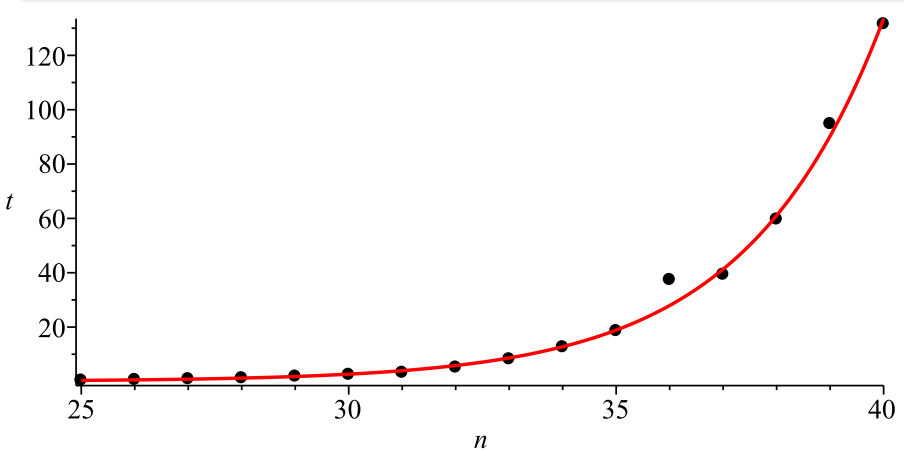
$t(60) \approx 4$ dny,

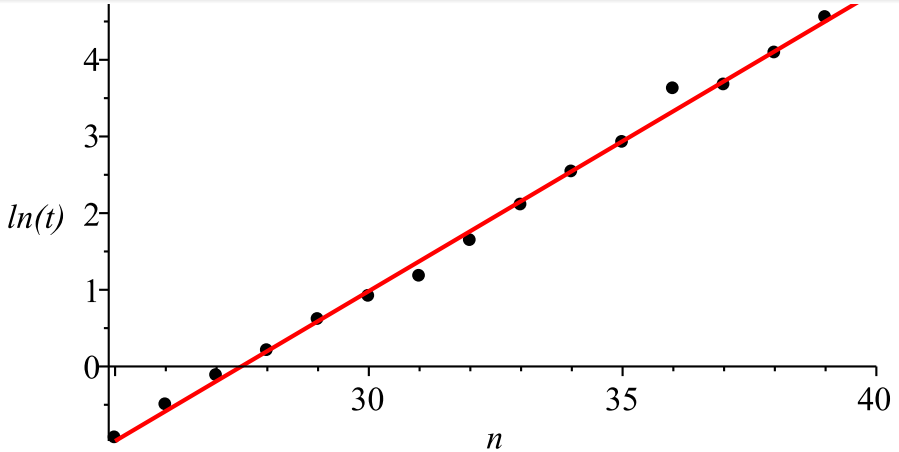
Naměřené časy





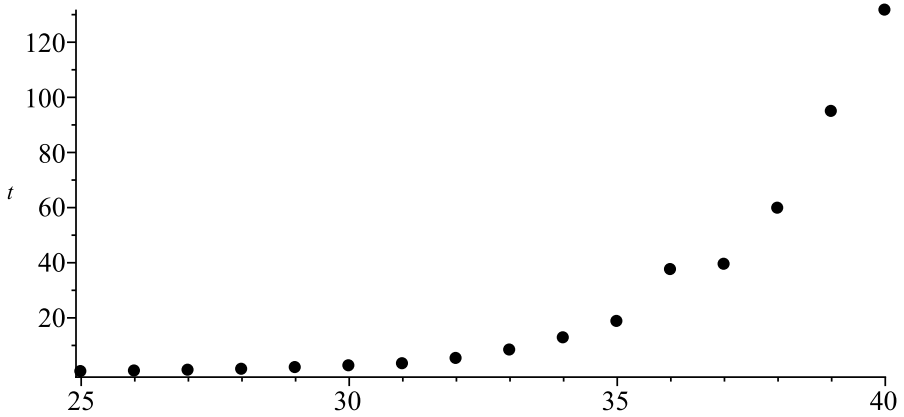
$t(n) \approx 0.000021408867798\, e^{0.391154069618199n}$

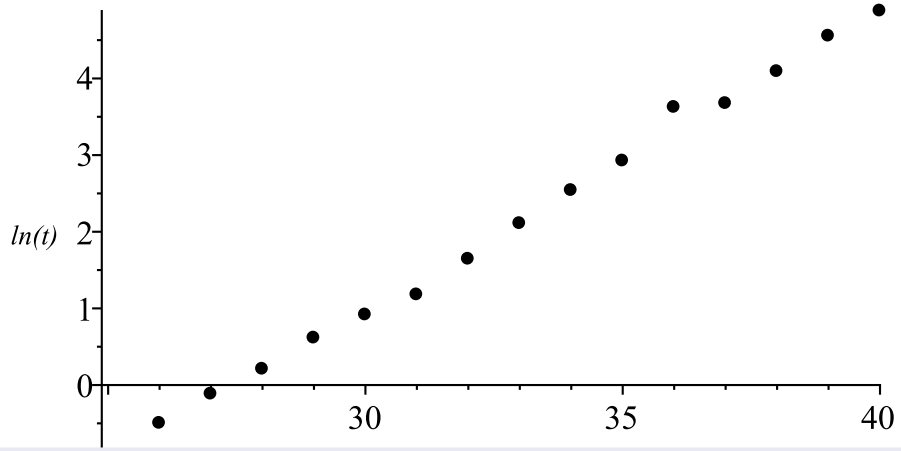




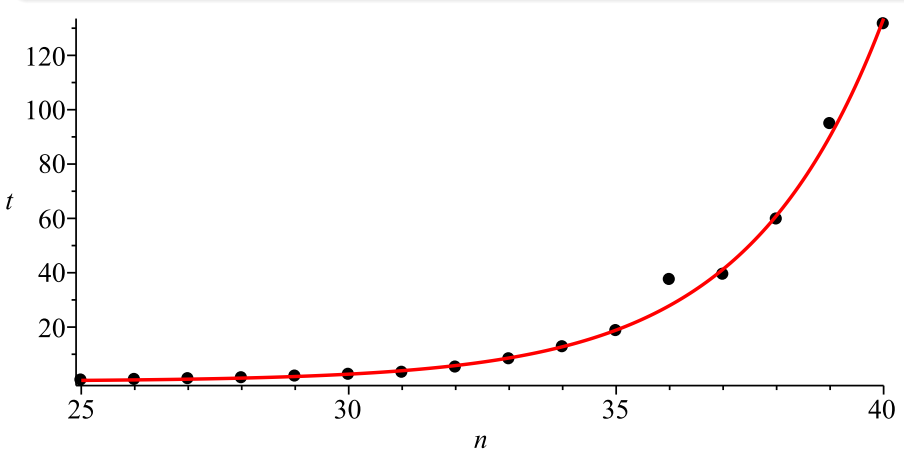
$t(60) \approx 4$ dny, $t(70) \approx 193$ dní,

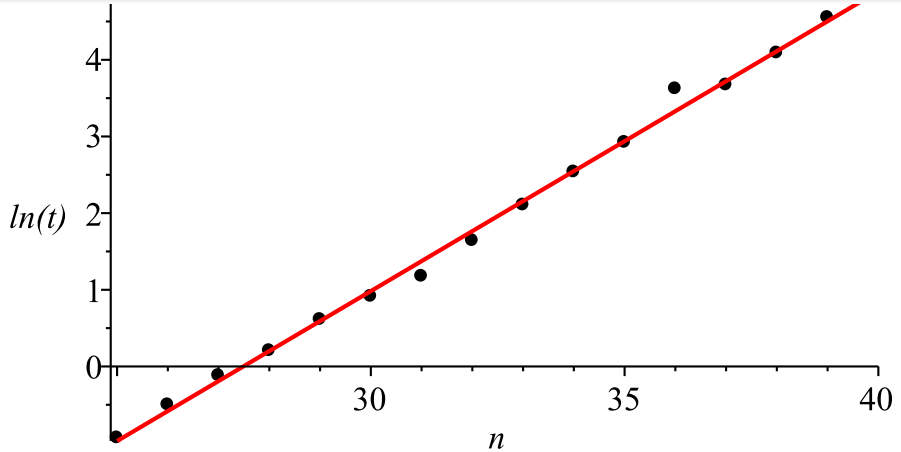
Naměřené časy





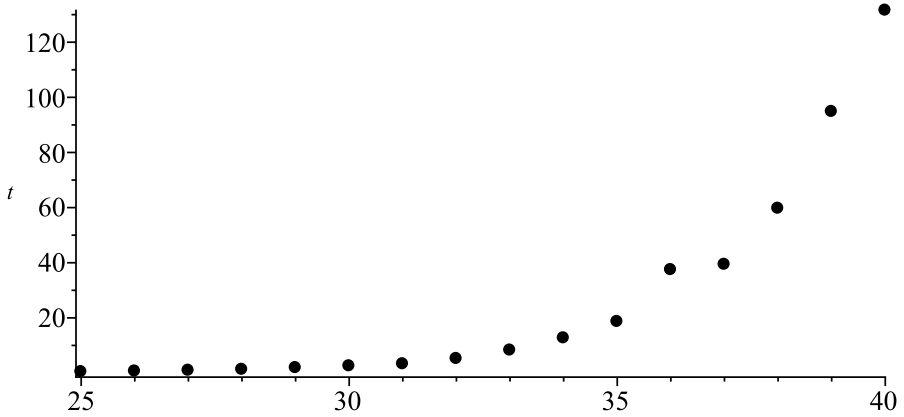
$t(n) \approx 0.000021408867798\, e^{0.391154069618199n}$

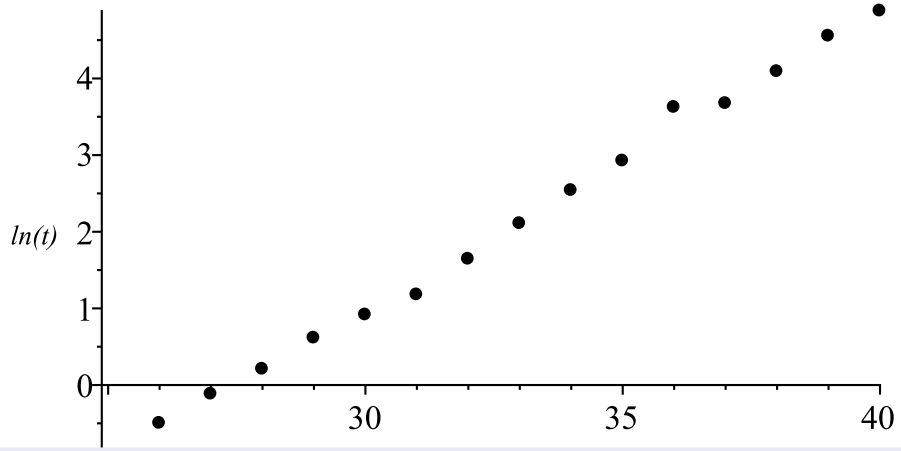




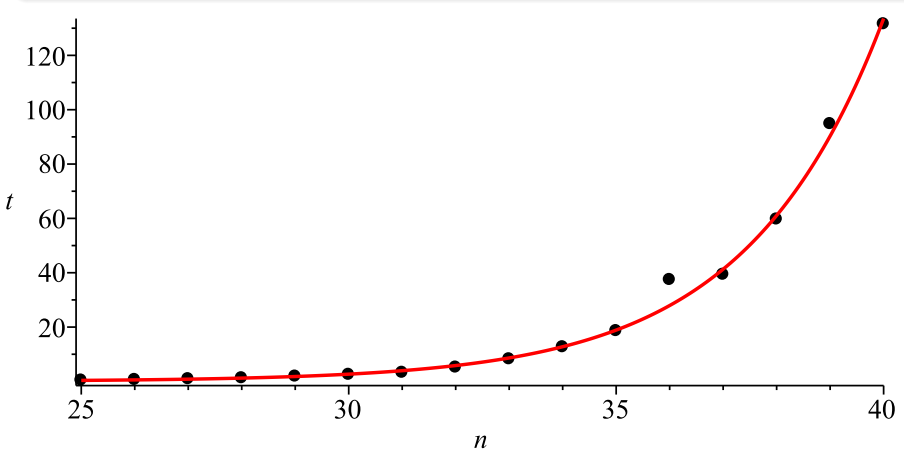
$t(60) \approx 4$ dny, $t(70) \approx 193$ dní, $t(80) \approx 26$ let,

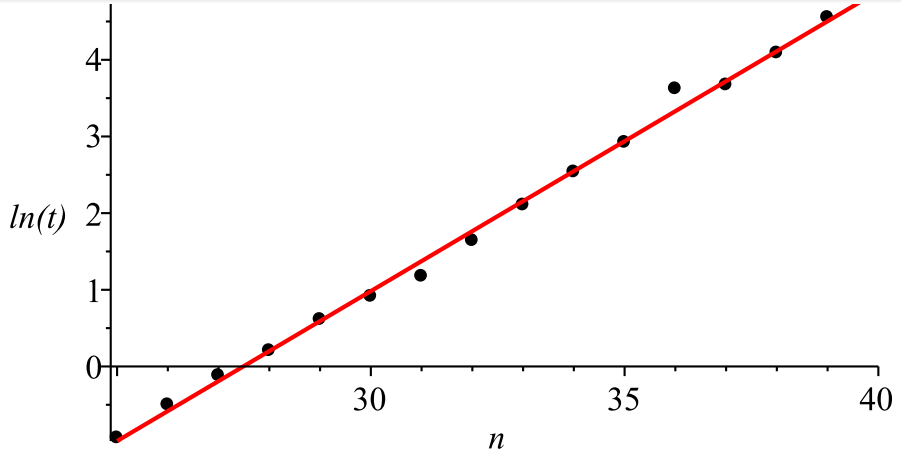
Naměřené časy





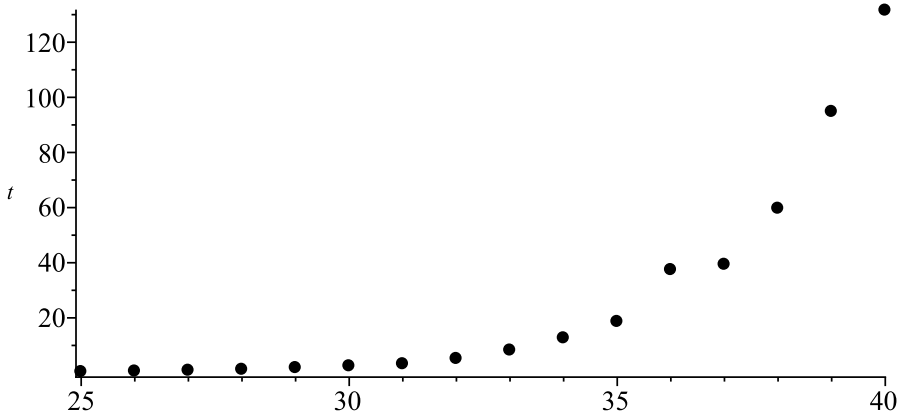
$t(n) \approx 0.000021408867798\, e^{0.391154069618199n}$

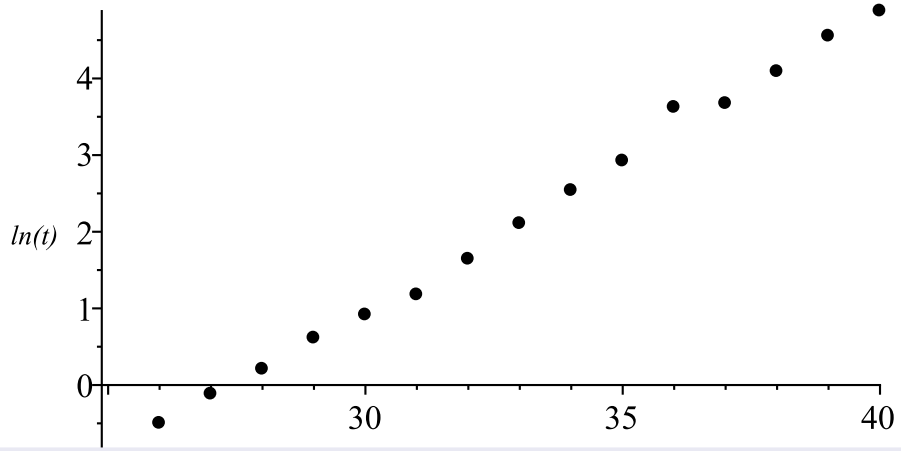




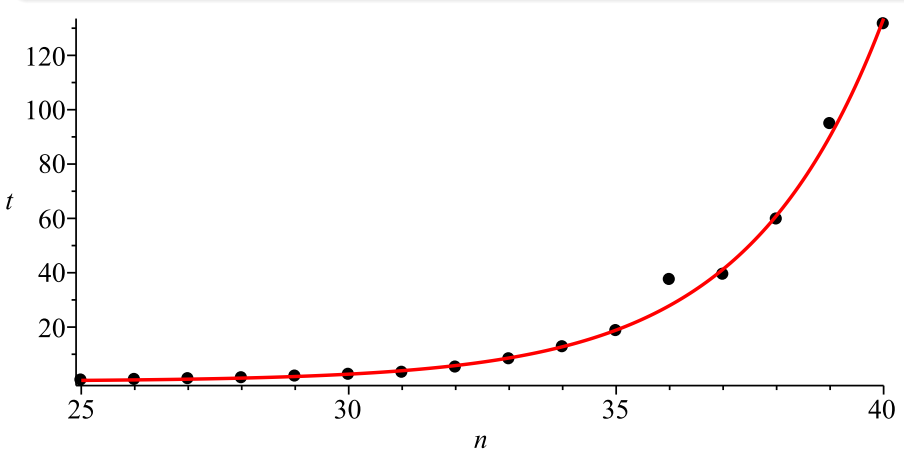
$t(60) \approx 4$ dny, $t(70) \approx 193$ dní, $t(80) \approx 26$ let, $t(90) \approx 1320$ let,

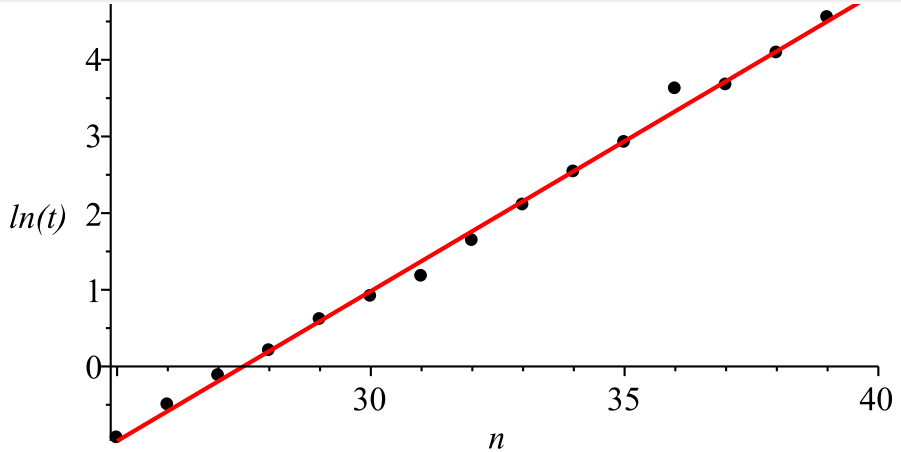
Naměřené časy





$t(n) \approx 0.000021408867798\, e^{0.391154069618199n}$

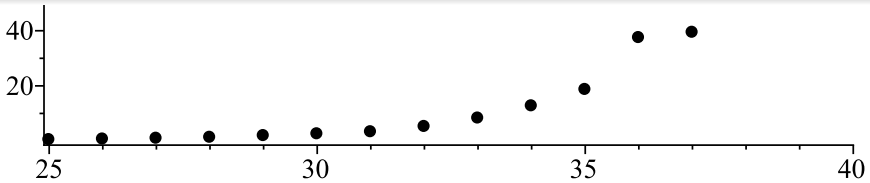


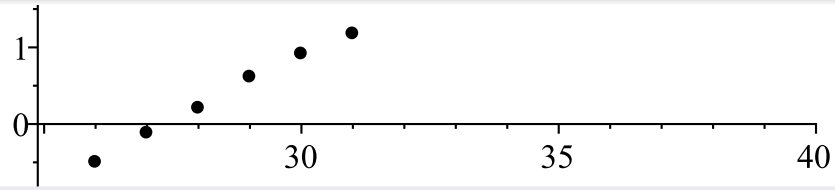


$t(60) \approx 4$ dny, $t(70) \approx 193$ dní, $t(80) \approx 26$ let, $t(90) \approx 1320$ let, $t(100) \approx 66\,000$ let.

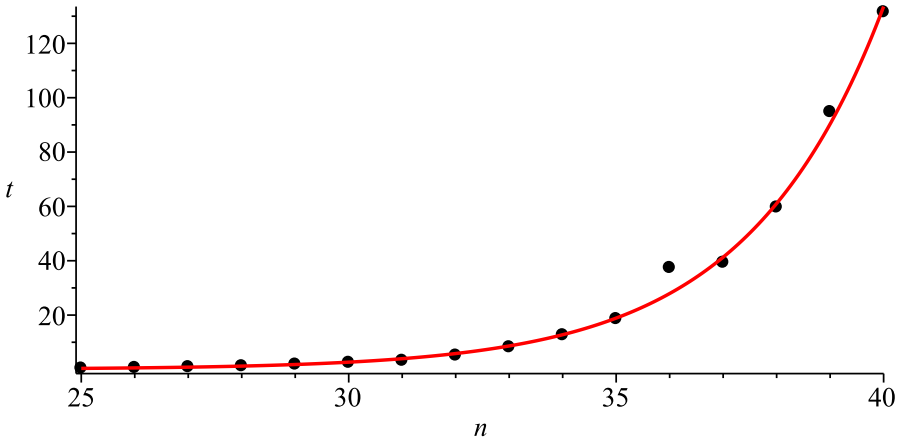
Naměřené časy

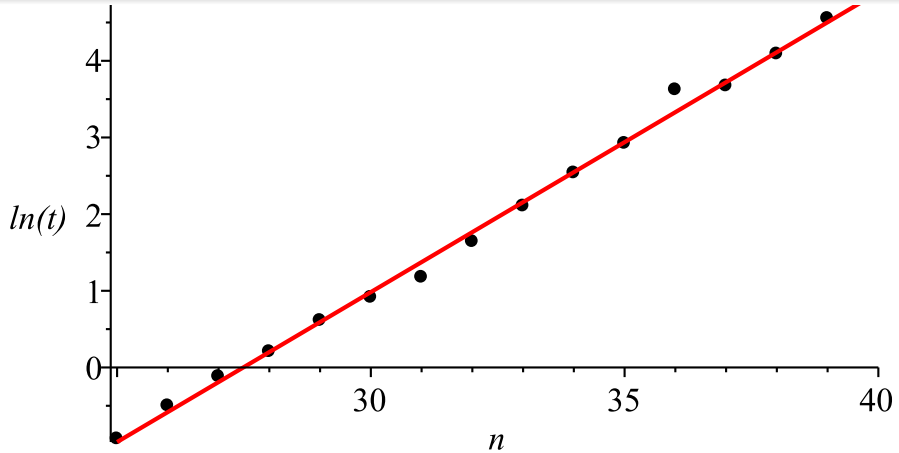
Procesor	12th Gen Intel(R) Core(TM) i7-1255U 1.70 GHz
Nainstalovaná paměť RAM	16,0 GB (použitelné: 15,7 GB)





$t(n) \approx 0.000021408867798\, e^{0.391154069618199n}$





$t(60) \approx 4$ dny, $t(70) \approx 193$ dní, $t(80) \approx 26$ let, $t(90) \approx 1320$ let, $t(100) \approx 66\,000$ let.

Děkuji za pozornost !!!