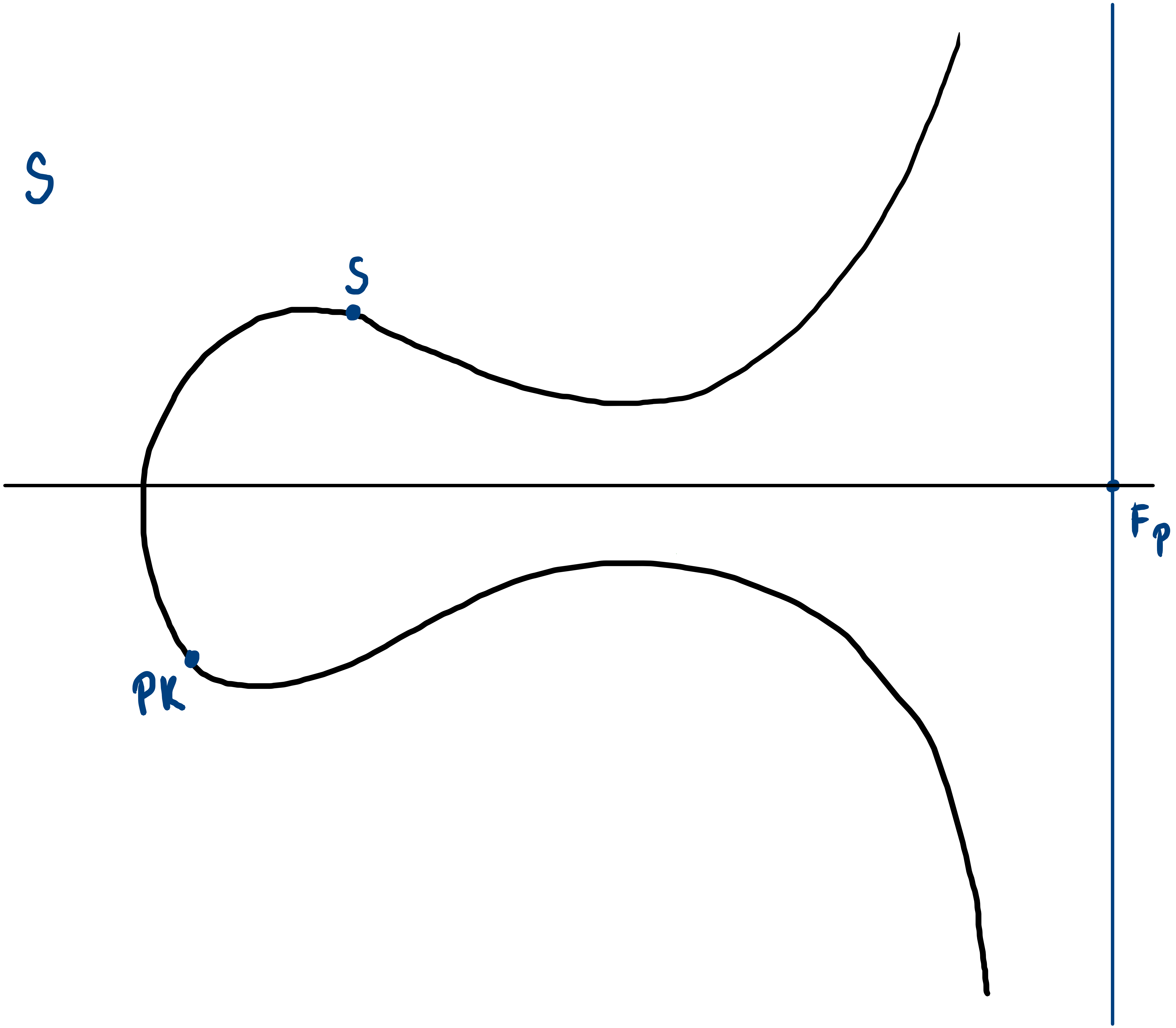
KRY - projekt 2 : ECC

Jak to funguje ?

Zadáno

- EC
- starting point S
- F_p
- PK

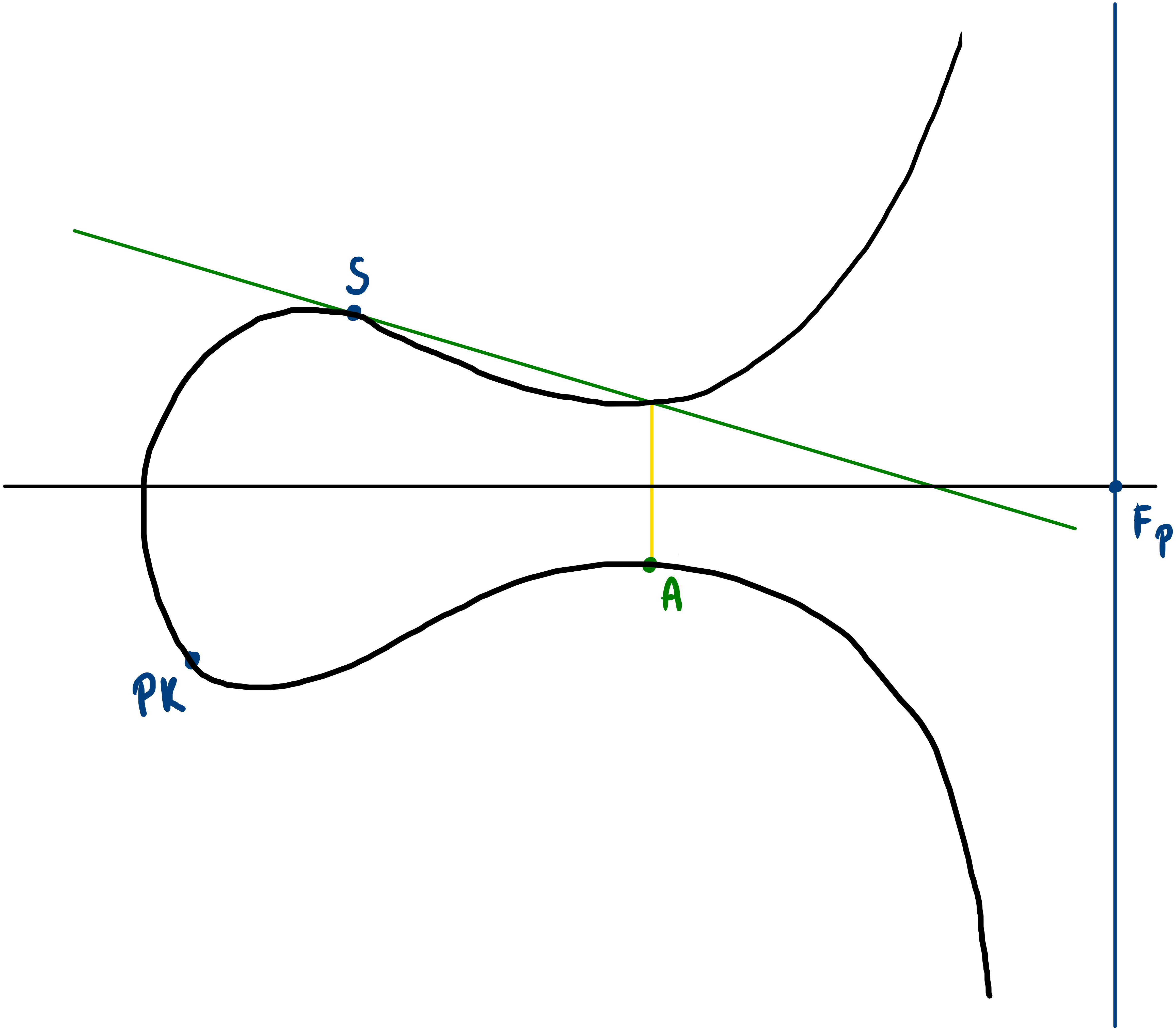


Hledáme

- SK = n

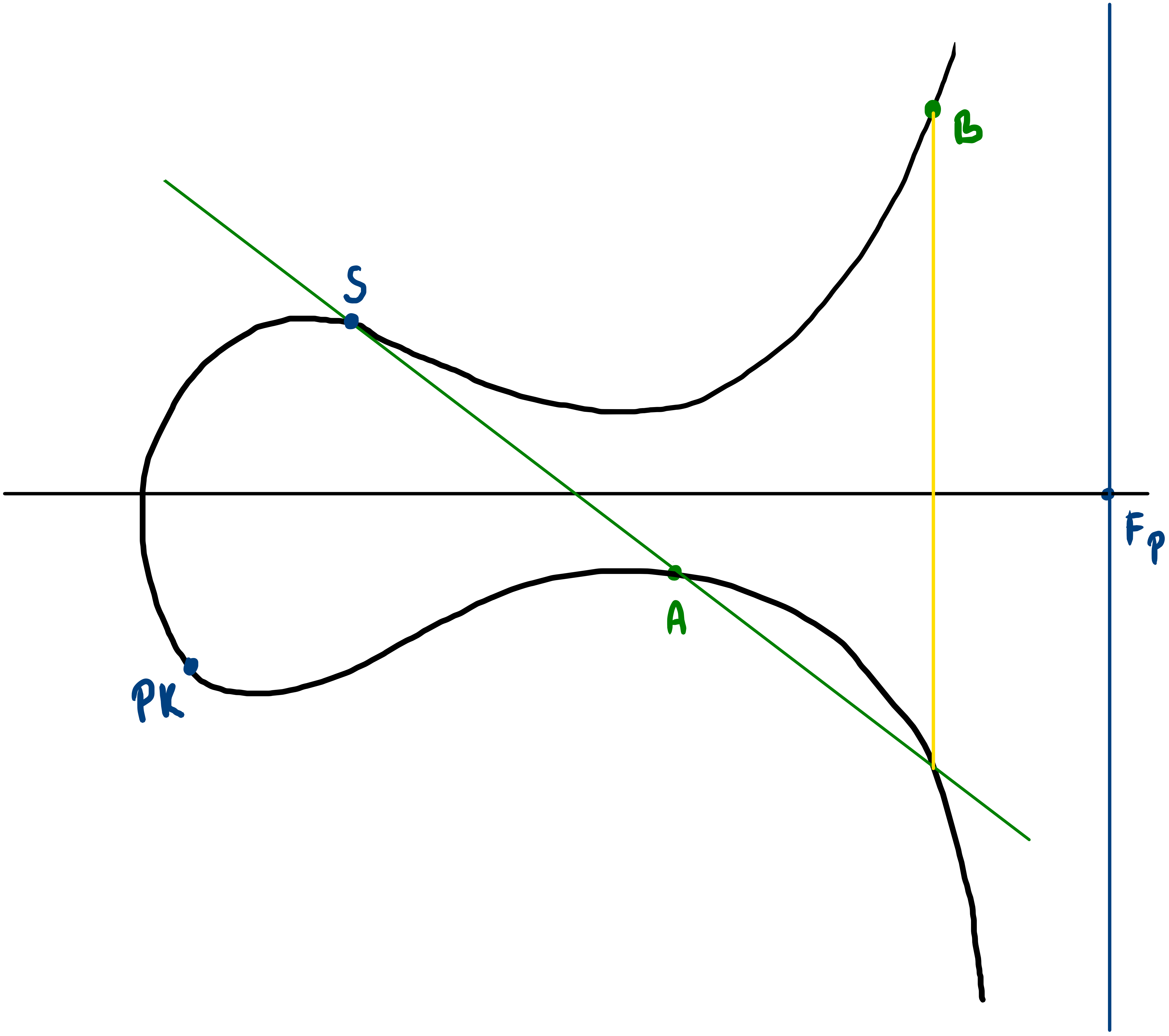
$n = 1$

$A \neq PK$



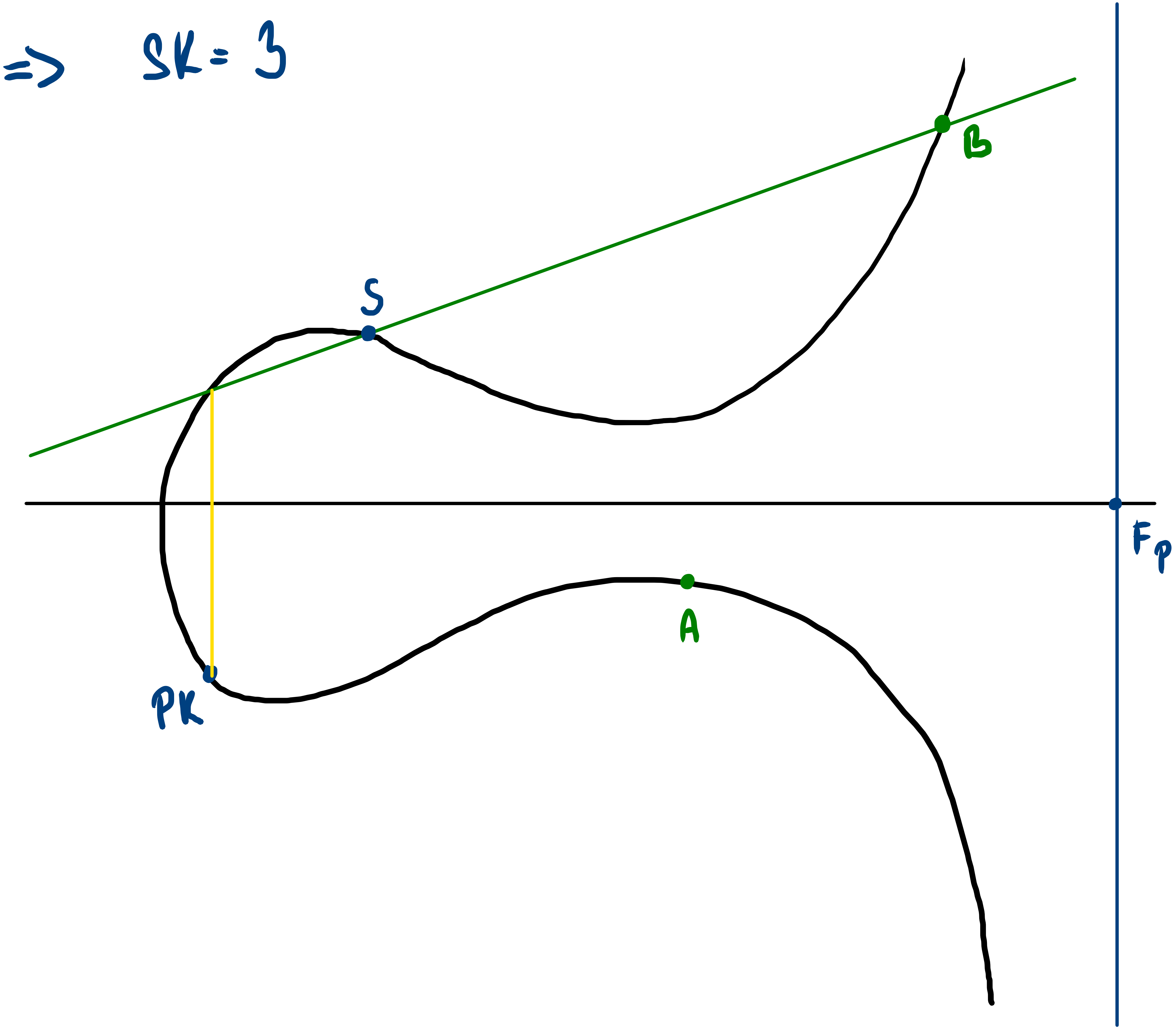
$n = 2$

$B \neq PK$



$n = 3 \Rightarrow SK = 3$

$C = PK$



Jak spočítat společné body přímky a EC

EC: $y^2 = x^3 + ax + b$ p: $y = cx + d$

$$y = \mp\sqrt{x^3+ax+b}$$

$$\mp\sqrt{x^3+ax+b} = cx+d$$

$$x^3+ax+b = c^2x^2+2cdx+d^2$$

$$x^3 - c^2x^2 + ax - 2cdx + b - d^2 = 0$$

$$x^3 - c^2x^2 + (a-2cd)\,x + b - d^2 = 0$$

Jak redukovat kubickou rovnici na kvadratickou, když známe kořen

$ax^3 + bx^2 + cx + d = 0$; $r_1 \in K$; $a, b, c, d \in \mathbb{Z}$

$(ax^3 + bx^2 + cx + d) : (x - r_1) = ax^2 + (b + r_1 a)x +$

$+ c + r_1 b + r_1^2 a$

$ax^3 - (ax^2 \cdot x) + (bx^2 - (-r_1 ax^2)) + cx + d$

$(b + r_1 a)x^2 + cx + d$

$0 + (cx - (-r_1 (b + r_1 a)x)) + d$

$cx - (-r_1 bx - r_1^2 ax) + d$

$(c + r_1 b + r_1^2 a)x + d$

$0 + (d - (-r_1 (c + r_1 b + r_1^2 a)))$

$d - (-r_1 c - r_1^2 b - r_1^3 a)$

$d + r_1 c + r_1^2 b + r_1^3 a$

Př. $x^3 - 2x^2 - 31x - 28 = 0$; $-1 \in K$

zbytek:

$$d + r_1 c + r_1^2 b + r_1^3 a$$

$$-28 - 1\cdot(-31) + (-1)^2\cdot(-2) + (-1)^3\cdot 1$$

$$= 0$$ ✓

Výsledek

$$ax^2 + (b + r_1 a)x + c + r_1 b + r_1^2 a$$

$$x^2 + (-2 - 1\cdot 1)x - 31 - 1(-2) + (-1)^2\cdot 1$$

$$x^2 - 3x - 28 = 0$$ ✓