Angewandte Mathematik

Übung 6.1

Christian Weißenbacher if19b127

1.)

1.) a) $y^2 = x^3 + ax + b$ $a = -2$

$y^2 = x^3 - 2x + 4$ $b = 4$

$4a^3 + 27b^2 \neq 0$

$4 \cdot (-2)^3 + 27 \cdot 4^2 = 400 \neq 0$

A: Sorgt dafür, dass $y^2 = x^3 + ax + b$ eine kommutative Gruppe ist

b)

x	± y
0	2
1	1,73
2	2,83
3	5
4	7,7
5	10,9
6	14,4

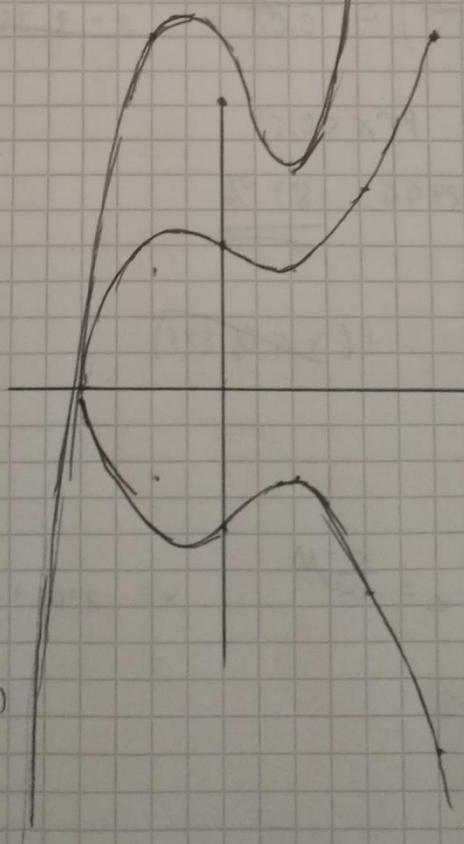
$y^2 = 0^3 + 2 \cdot 0 + 4$

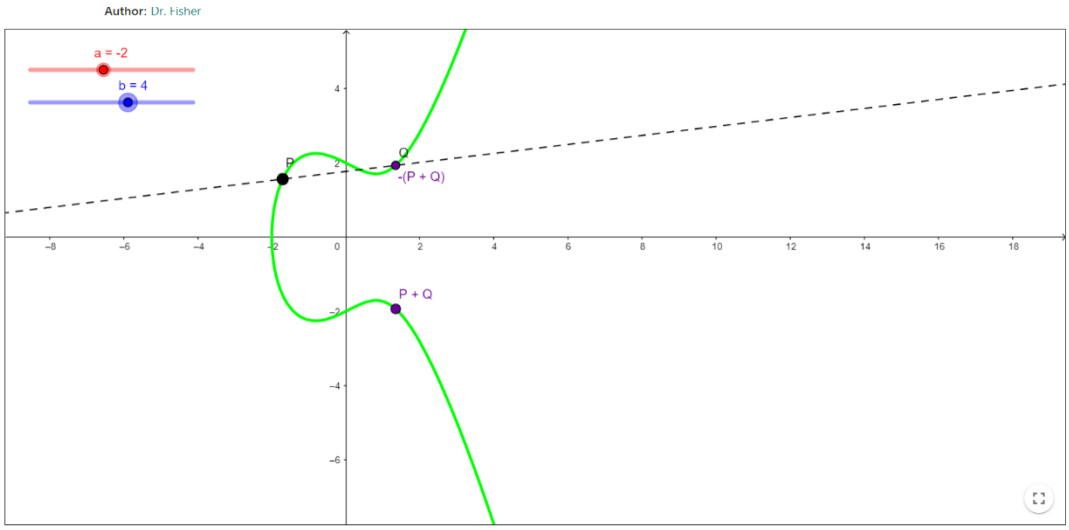
$y^2 = 4$ $y = \sqrt{4} = \pm 2$

c) kubisches Polynom

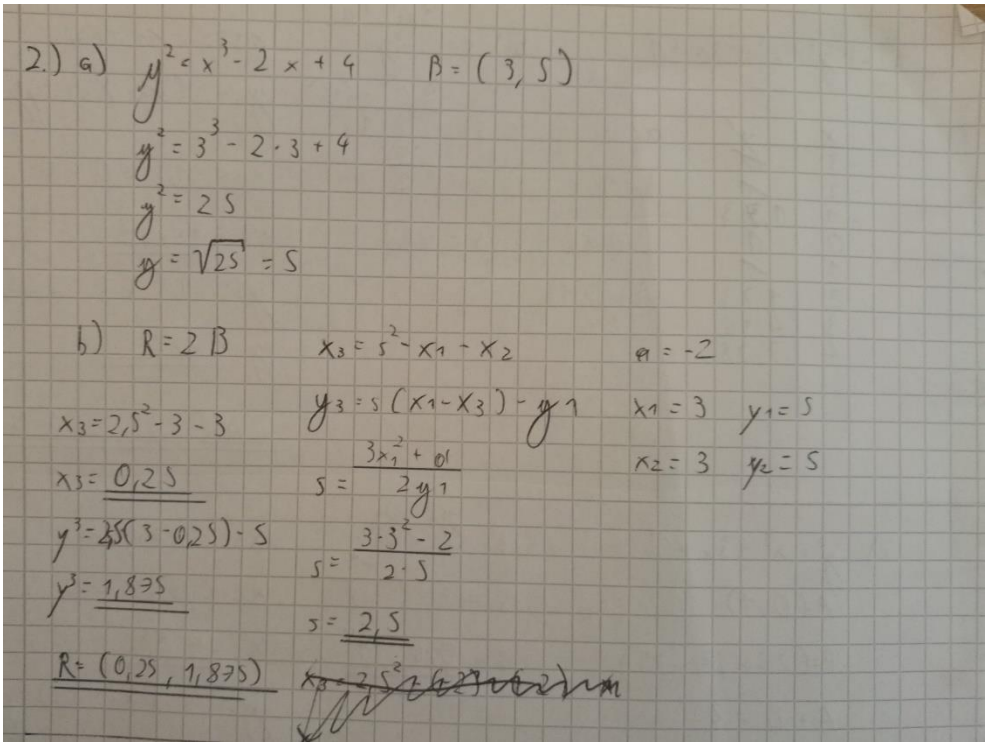
$p(x) = x^3 - 2x + 4$

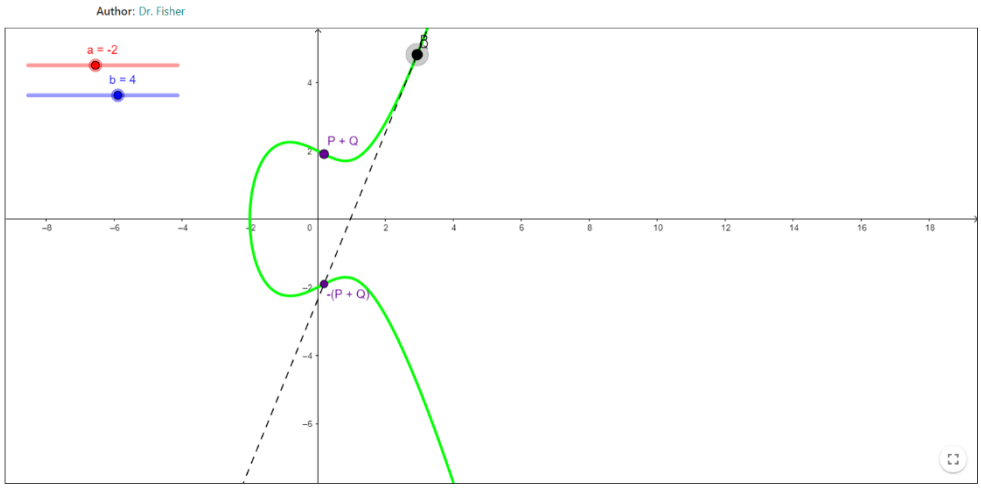
x	p(x)
-3	-17
-2	0
-1	5
0	4
1	3
2	8
3	25



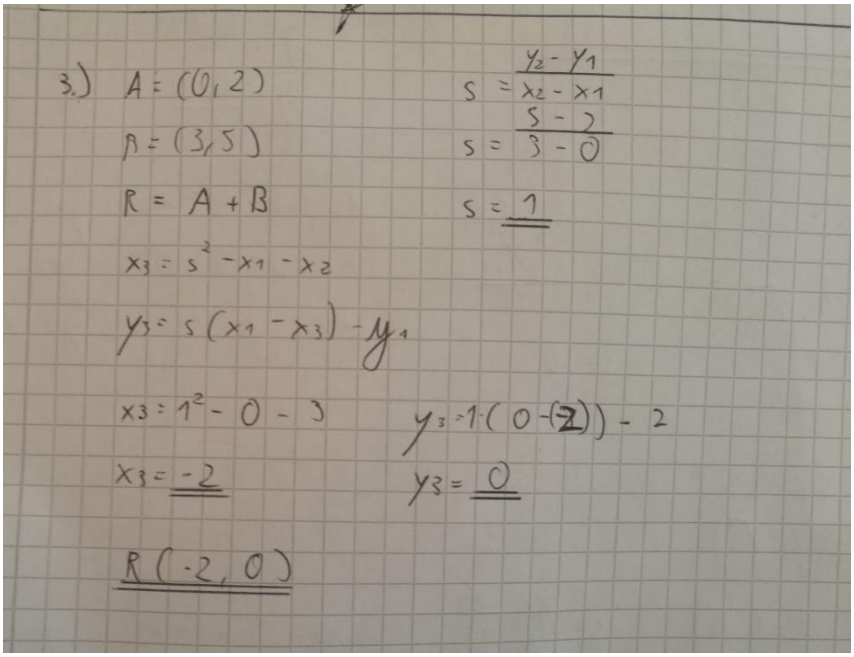

Author: Dr. Fisher
a = -2
b = 4
P
Q
-(P + Q)
P + Q

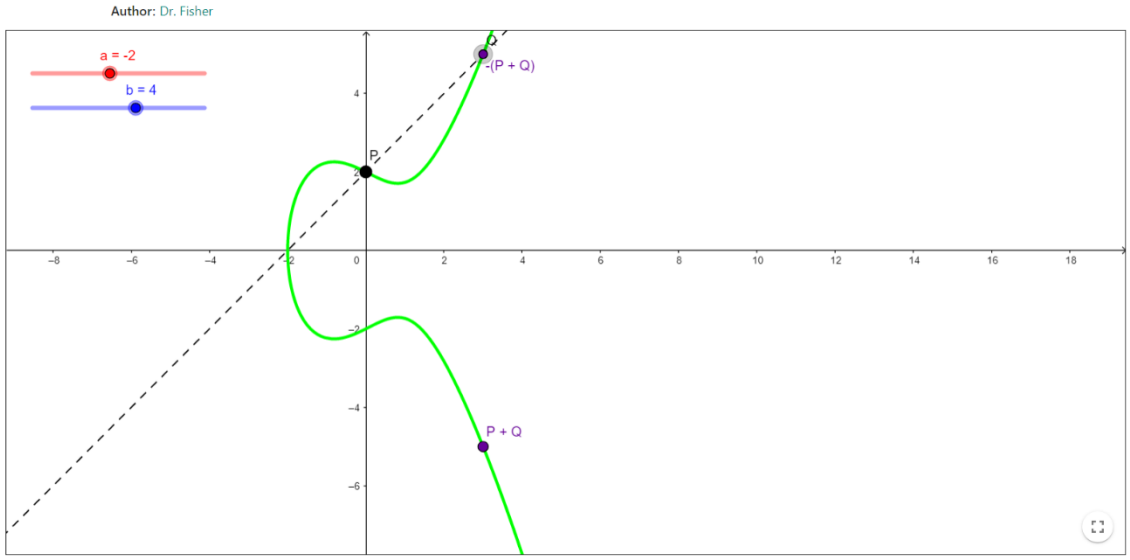
2.)


2.) a) $y^2 = x^3 - 2x + 4$ $B = (3, 5)$
$y^2 = 3^3 - 2 \cdot 3 + 4$
$y^2 = 25$
$y = \sqrt{25} = 5$
b) $R = 2B$
$x_3 = s^2 - x_1 - x_2$
$y_3 = s(x_1 - x_3) - y_1$
$s = \frac{3x_1^2 + a}{2y_1}$
$s = \frac{3 \cdot 3^2 - 2}{2 \cdot 5}$
$s = 2,5$
$x_3 = 2,5^2 - 3 - 3$
$x_3 = 0,25$
$y^3 = 2,5(3 - 0,25) - 5$
$y^3 = 1,875$
$R = (0,25; 1,875)$
$a = -2$
$x_1 = 3$ $y_1 = 5$
$x_2 = 3$ $y_2 = 5$

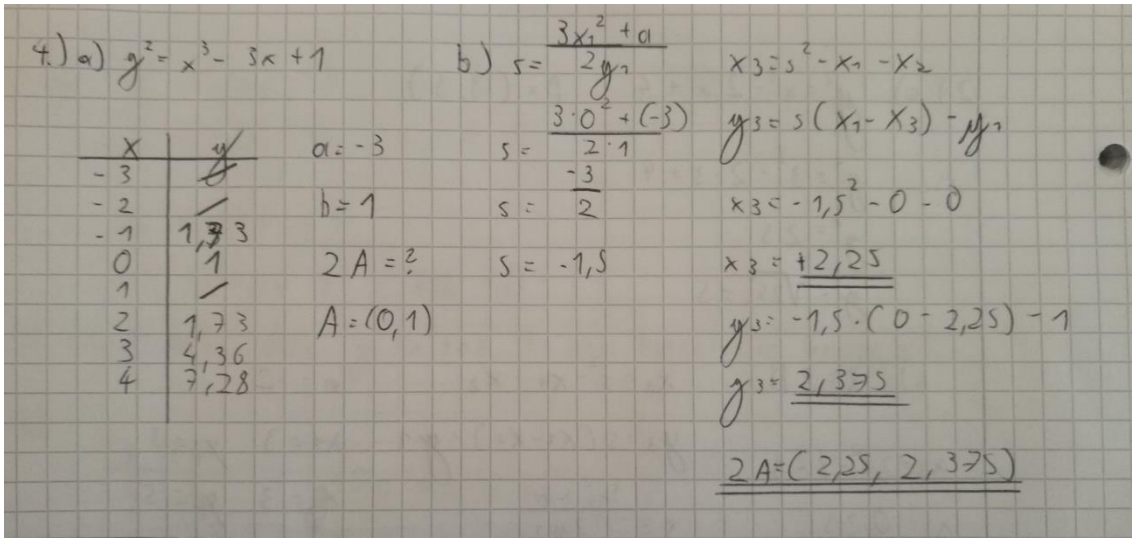

Author: Dr. Fisher
a = -2
b = 4
B
P + Q
-(P + Q)

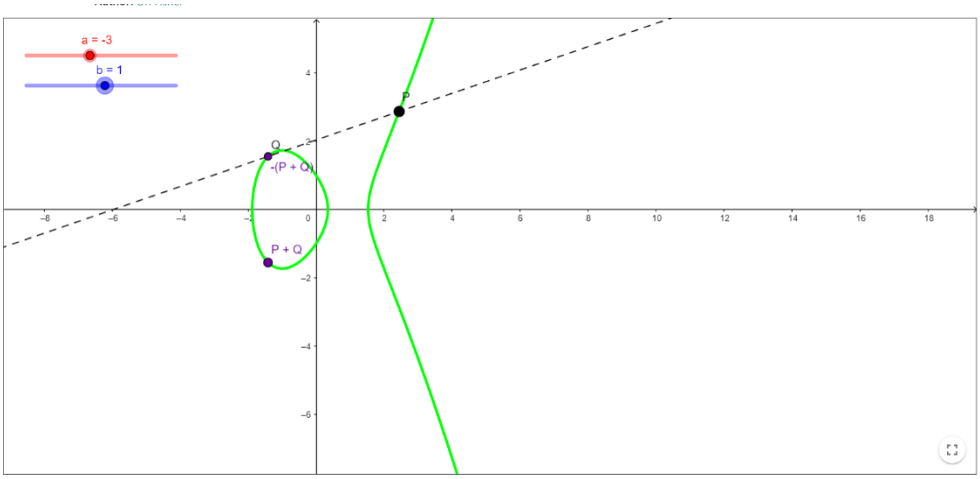
3.)

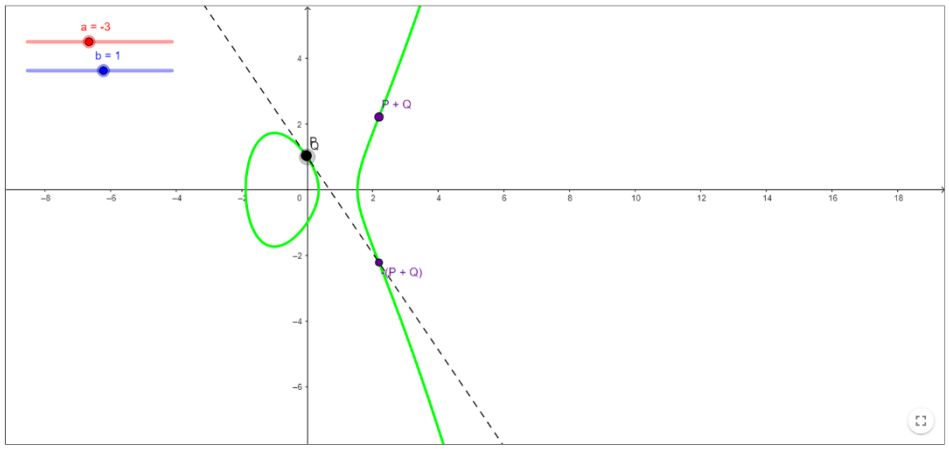

3.) A = (0, 2)
B = (3, 5)
R = A + B
$x_3 = s^2 - x_1 - x_2$
$y_3 = s(x_1 - x_3) - y_1$
$x_3 = 1^2 - 0 - 3$
$x_3 = -2$
R (-2, 0)
$s = \frac{y_2 - y_1}{x_2 - x_1}$
$s = \frac{5 - 2}{3 - 0}$
$s = 1$
$y_3 = 1 \cdot (0 - (-2)) - 2$
$y_3 = 0$


Author: Dr. Fisher
a = -2
b = 4
Q
-(P + Q)
P
P + Q

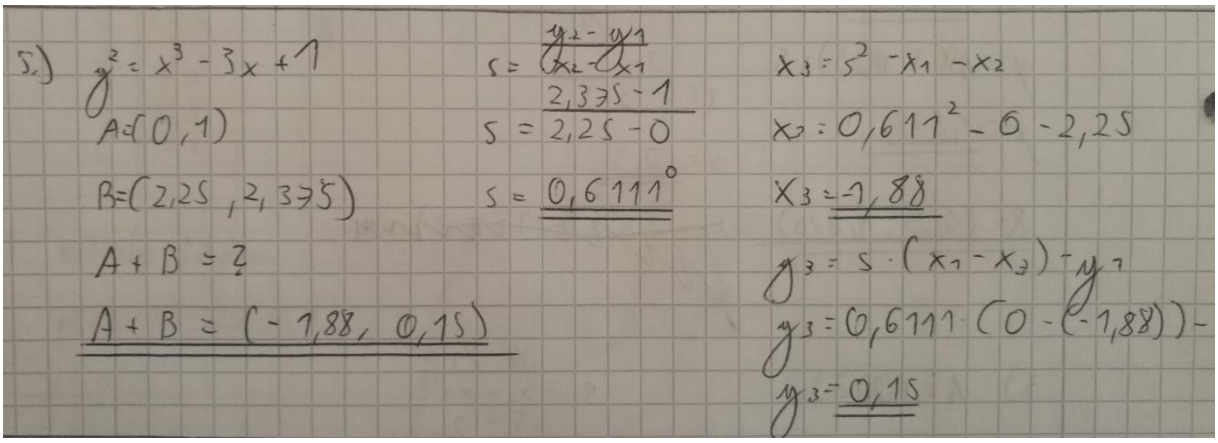
4.)

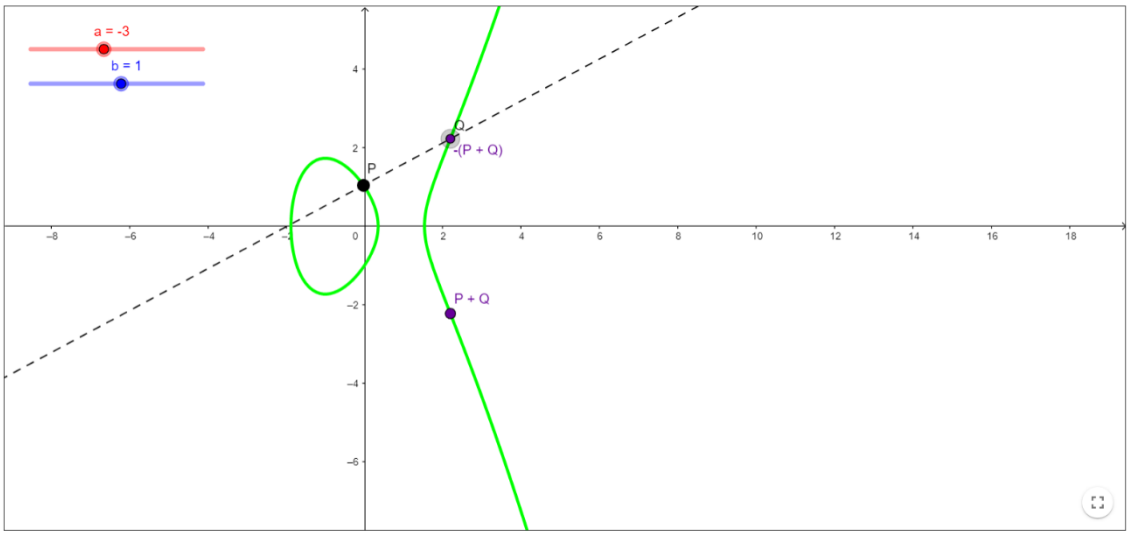

4.) a) $y^2 = x^3 - 3x + 1$
b) $s = \frac{3x_1^2 + a}{2y_1}$
$x_3 = s^2 - x_1 - x_2$
$y_3 = s(x_1 - x_3) - y_1$
a = -3
b = 1
2A = ?
A = (0,1)
$s = \frac{3 \cdot 0^2 + (-3)}{2 \cdot 1}$
$s = \frac{-3}{2}$
$s = -1,5$
$x_3 = -1,5^2 - 0 - 0$
$x_3 = 2,25$
$y_3 = -1,5 \cdot (0 - 2,25) - 1$
$y_3 = 2,375$
2A = (2,25; 2,375)


a = -3
b = 1
P
Q
-(P + Q)
P + Q

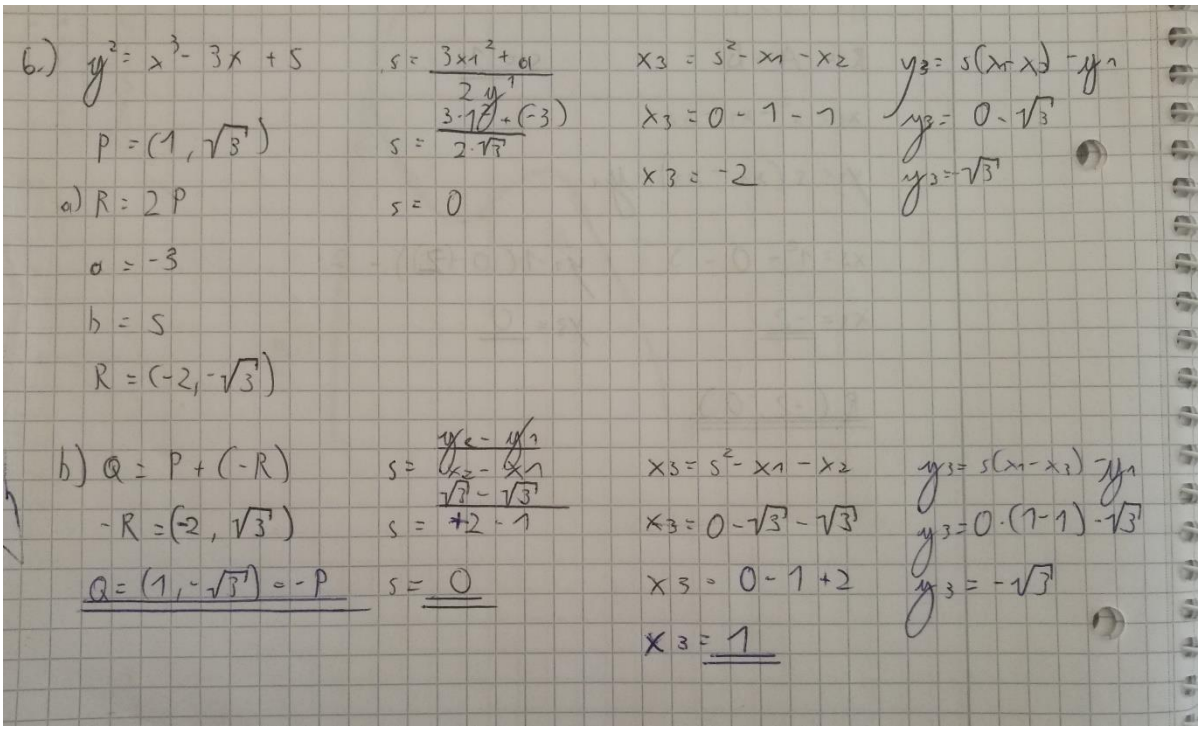

a = -3
b = 1
P + Q
B
-(P + Q)

5.)

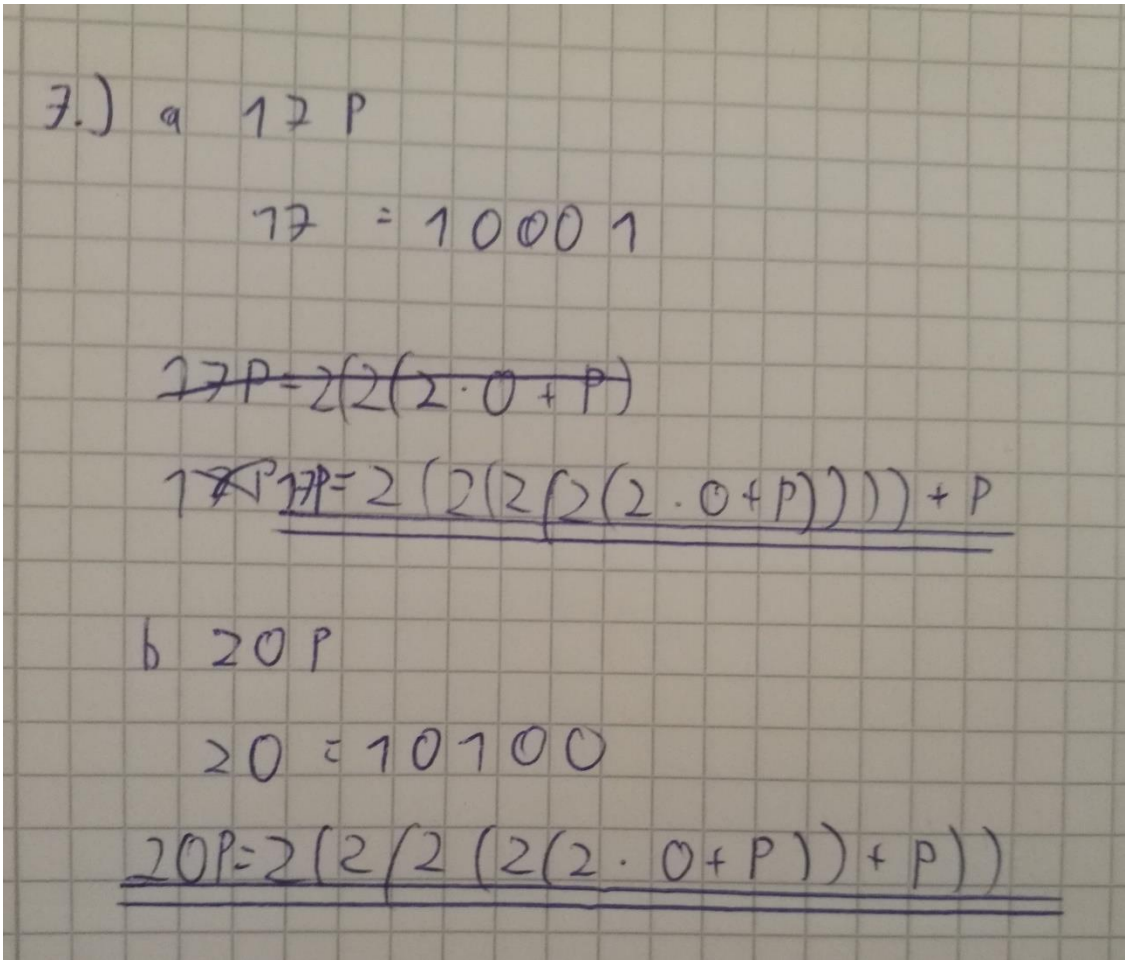

5.) $y^2 = x^3 - 3x + 1$
A=(0,1)
B=(2,25 , 2,375)
A + B = ?
A + B = (-1,88, 0,15)
$s = \frac{y_2 - y_1}{x_2 - x_1}$
$s = \frac{2,375 - 1}{2,25 - 0}$
$s = 0,6111^{\circ}$
$x_3 = s^2 - x_1 - x_2$
$x_3 = 0,611^2 - 0 - 2,25$
$x_3 = -1,88$
$y_3 = s \cdot (x_1 - x_3) - y_1$
$y_3 = 0,6111 \cdot (0 - (-1,88)) -$
$y_3 = 0,15$


a = -3
b = 1
P
Q
-(P + Q)
P + Q

6.)


6.) $y^2 = x^3 - 3x + 5$
P = (1, $\sqrt{3}$)
a) R = 2P
a = -3
b = 5
R = (-2, $-\sqrt{3}$)
b) Q = P + (-R)
-R = (-2, $\sqrt{3}$)
Q = (1, $-\sqrt{3}$) = -P
$s = \frac{3x_1^2 + a}{2y_1}$
$s = \frac{3 \cdot 1^2 + (-3)}{2 \cdot \sqrt{3}}$
s = 0
$s = \frac{y_2 - y_1}{x_2 - x_1}$
$s = \frac{\sqrt{3} - \sqrt{3}}{+2 - 1}$
s = 0
$x_3 = s^2 - x_1 - x_2$
$x_3 = 0 - 1 - 1$
$x_3 = -2$
$x_3 = s^2 - x_1 - x_2$
$x_3 = 0 - \sqrt{3} - \sqrt{3}$
$x_3 = 0 - 1 + 2$
$x_3 = 1$
$y_3 = s(x_1 - x_3) - y_1$
$y_3 = 0 - \sqrt{3}$
$y_3 = -\sqrt{3}$
$y_3 = s(x_1 - x_3) - y_1$
$y_3 = 0 \cdot (1 - 1) - \sqrt{3}$
$y_3 = -\sqrt{3}$

7.)



7.) a 17 P

17 = 10001

~~17P = 2(2(2 · 0 + P)~~

~~17P~~ 17P = 2(2(2(2(2 · 0 + P)))) + P

b 20 P

20 = 10100

20P = 2(2(2(2(2 · 0 + P)) + P))