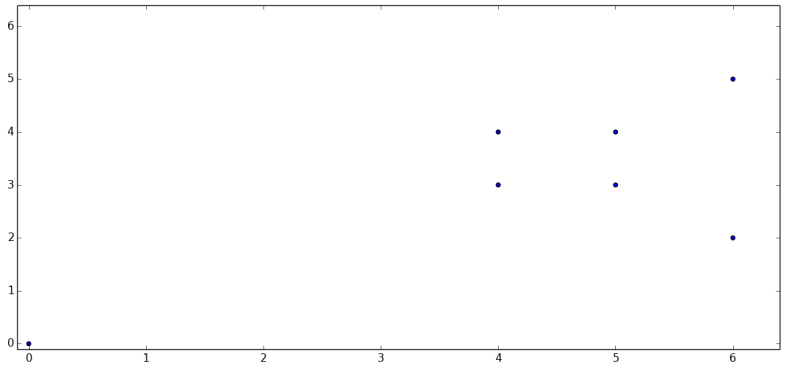
Kryptografian alkeet
5. harjoitukset, ratkaisuja
Jesse Jääsaari (jesse.jaasaari@helsinki.fi)

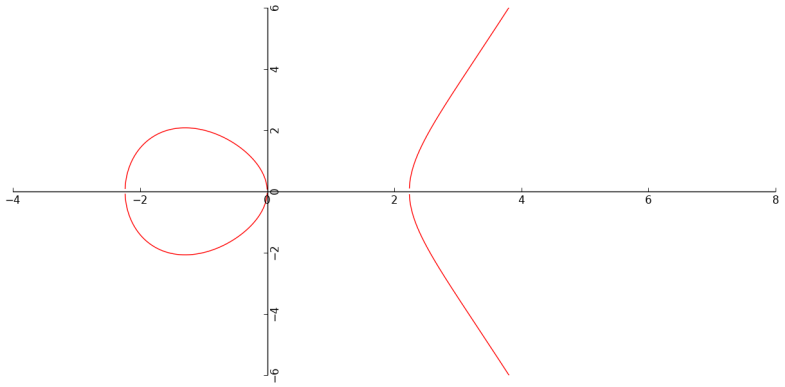
1. Piirrä käyrän $y^2 = x^3 - 5x$ kuvaaja modulossa 7 ja hahmottele se reaalilukujen joukossa.

Ratkaisu. Lasketaan ensin käyrän pisteet modulo 7:

$x \pmod 7$	$x^3 - 5x \pmod 7$
0	$0 \equiv 0^2$
1	3, neliönepäjäännös
2	5, neliönepäjäännös
3	5, neliönepäjäännös
4	$2 \equiv 3^2 \equiv 4^2$
5	$9 \equiv 3^2 \equiv 4^2$
6	$4 \equiv 2^2 \equiv 5^2$

Tästä nähdään, että elliptisen käyrän pisteet modulo 7 ovat $(0,0), (4,3), (4,4), (5,3), (5,4), (6,2)$, ja $(6,5)$. Alla käyrän kuvaajat modulo 7 ja reaalilukujen joukossa.





2. Arvioi ykköstehtävän karkeasti piirroksesi perusteella, mikä on pisteiden $P = (0, 0)$ ja $Q = (-1, 2)$ summa. Laske näiden pisteiden summa kaavan avulla reaalilukutilanteessa.

Ratkaisu. Pisteiden $P =: (x_P, y_P)$ ja $Q =: (x_Q, y_Q)$ summa saadaan seuraavasti: piirretään ensin näiden pisteiden kautta kulkeva suora. Se leikkaa käyrän jossakin kolmannessa pisteessä. Kysytty summapiste on tämän pisteen peilaus x-akselin yli. Hyvästä piirroksesta voi päätellä pisteen olevan $(5, 10)$. Lasketaan sitten summapiste kaavan avulla. Parametriksi s saadaan $(y_P - y_Q)/(x_P - x_Q) = (0-2)/(0-(-1)) = -2$. Nyt summapisteen x-koordinaatiksi saadaan $s^2 - x_P - x_Q = 4 - 0 + 1 = 5$ ja y-koordinaatiksi $-y_P + s(x_P - x_R) = 0 - 2(0-5) = 10$. Siis $P + Q = (5, 10)$.

3. Laske pisteiden $P = (0, 0)$ ja $Q = (-1, 2)$ summa kunnassa $\mathbb{Z}_7$.

Ratkaisu. Kaavat menevät samalla tavalla kuin tehtävässä 2, mutta nyt kaikki redusoidaan modulo 7. Koska edellisen tehtävän s sattuu olemaan kokonaisluku, niin summapisteeksi saadaan suoraan $(5, 3)$, onhan $5 \equiv 5 \pmod 7$ ja $10 \equiv 3 \pmod 7$.

4. Laske $2Q$ käyrällä $y^2 = x^3 - 5x$ sekä reaalilukujen joukossa että kunnassa $\mathbb{Z}_7$, kun $Q = (-1, 2)$.

Ratkaisu. Lasketaan $2Q =: (x_{2Q}, y_{2Q})$ ensin reaalilukujen joukossa. Määritetään parametri s:

$$s = \frac{3x_P^2 - 5}{2y_P} = \frac{3-5}{4} = -\frac{1}{2}.$$

Nyt $x_{2Q} = s^2 - 2x_Q = \frac{9}{4}$ ja $y_{2Q} = -y_Q + s(x_Q - x_R) = -\frac{3}{8}$. Siis $2Q = \left(\frac{9}{4}, -\frac{3}{8}\right)$.

Lasketaan $2Q$ sitten kunnassa $\mathbb{Z}_7$. Nyt

$$s = -\frac{1}{2} \equiv -4 \equiv 3 \pmod 7.$$

Tällöin $x_{2Q} = 9 + 2 \equiv 4 \pmod 7$ ja $y_{2Q} = -2 + 3(-1-4) = -17 \equiv 4 \pmod 7$. Siis kunnassa $\mathbb{Z}_7$ pätee $2Q = (4, 4)$.

5. Kohdat a ja b ovat vaihtoehtoisia:

(a) Piirrä tietokoneella elliptinen käyrä $y^2 = x^3 + 200x + 192$ kunnassa $\mathbb{Z}_{281}$ ja listaa sen pisteet.

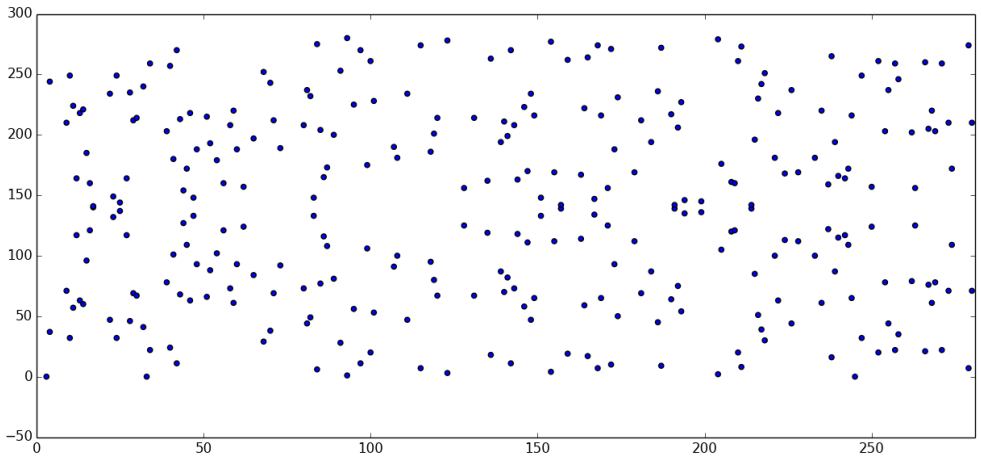
(b) Kunnan $\mathbb{Z}_{31}$ elliptisellä käyrällä on pisteet $(12, 3)$ ja $(1, 9)$. Etsi käyrä.

Ratkaisu. (a) Alla on luettelo käyrän pisteistä:

(3, 0) (4, 37), (4, 244), (9, 71), (9, 210), (10, 32), (10, 249), (11, 57), (11, 224), (12, 117), (12, 164), (13, 63), (13, 218), (14, 60), (14, 221), (15, 96), (15, 185), (16, 121), (16, 160), (17, 140), (17, 141), (22, 47), (22, 234), (23, 132), (23, 149), (24, 32), (24, 249), (25, 137), (25, 144), (27, 117), (27, 164), (28, 46), (28, 235), (29, 69), (29, 212), (30, 67), (30, 214), (32, 41), (32, 240), (33, 0), (34, 22), (34, 259), (39, 78), (39, 203), (40, 24), (40, 257), (41, 101), (41, 180), (42, 11), (42, 270), (43, 68), (43, 213), (44, 127), (44, 154), (45, 109), (45, 172), (46, 63), (46, 218), (47, 133), (47, 148), (48, 93), (48, 188), (51, 66), (51, 215), (52, 88), (52, 193), (54, 102), (54, 179), (56, 121), (56, 160), (58, 73), (58, 208), (59, 61), (59, 220), (60, 93), (60, 188), (62, 124), (62, 157), (65, 84), (65, 197), (68, 29), (68, 252), (70, 38), (70, 243), (71, 69), (71, 212), (73, 92), (73, 189), (80, 73), (80, 208), (81, 44), (81, 237), (82, 49), (82, 232), (83, 133), (83, 148), (84, 6), (84, 275), (85, 77), (85, 204), (86, 116), (86, 165), (87, 108), (87, 173), (89, 81), (89, 200), (91, 28), (91, 253), (93, 1), (93, 280), (95, 56), (95, 225), (97, 11), (97, 270), (99, 106), (99, 175), (100, 20), (100, 261), (101, 53), (101, 228), (107, 91), (107, 190), (108, 100), (108, 181), (111, 47), (111, 234), (115, 7), (115, 274), (118, 95), (118, 186), (119, 80), (119, 201), (120, 67), (120, 214), (123, 3), (123, 278), (128, 125), (128, 156), (131,

67), (131, 214), (135, 119), (135, 162), (136, 18), (136, 263), (139, 87), (139, 194), (140, 70), (140, 211), (141, 82), (141, 199), (142, 11), (142, 270), (143, 73), (143, 208), (144, 118), (144, 163), (146, 58), (146, 223), (147, 111), (147, 170), (148, 47), (148, 234), (149, 65), (149, 216), (151, 133), (151, 148), (154, 4), (154, 277), (155, 112), (155, 169), (157, 139), (157, 142), (159, 19), (159, 262), (163, 114), (163, 167), (164, 59), (164, 222), (165, 17), (165, 264), (167, 134), (167, 147), (168, 7), (168, 274), (169, 65), (169, 216), (171, 125), (171, 156), (172, 10), (172, 271), (173, 93), (173, 188), (174, 50), (174, 231), (179, 112), (179, 169), (181, 69), (181, 212), (184, 87), (184, 194), (186, 45), (186, 236), (187, 9), (187, 272), (190, 64), (190, 217), (191, 139), (191, 142), (192, 75), (192, 206), (193, 54), (193, 227), (194, 135), (194, 146), (199, 136), (199, 145), (204, 2), (204, 279), (205, 105), (205, 176), (208, 120), (208, 161), (209, 121), (209, 160), (210, 20), (210, 261), (211, 8), (211, 273), (214, 139), (214, 142), (215, 85), (215, 196), (216, 51), (216, 230), (217, 39), (217, 242), (218, 30), (218, 251), (221, 100), (221, 181), (222, 63), (222, 218), (224, 113), (226, 44), (226, 237), (228, 112), (228, 169), (233, 100), (233, 181), (235, 61), (235, 220), (237, 122), (237, 159), (238, 16), (238, 265), (239, 87), (239, 194), (240, 115), (240, 166), (242, 117), (242, 164), (243, 109), (243, 172), (244, 65), (244, 216), (245, 0), (247, 32), (247, 249), (250, 124), (250, 157), (252, 20), (252, 261), (254, 78), (254, 203), (255, 44), (255, 237), (257, 22), (257, 259), (258, 35), (258, 246), (262, 79), (262, 202), (263, 125), (263, 156), (266, 21), (266, 260), (267, 76), (267, 205), (268, 61), (268, 220), (269, 78), (269, 203), (271, 22), (271, 259), (273, 71), (273, 210), (274, 109), (274, 172), (279, 7), (279, 274), (280, 71), (280, 210).

Pisteet asettuvat seuraavasti:



(b) Koska pisteet $(12, 3)$ ja $(1, 9)$ ovat elliptisellä käyrällä $y^2 = x^3 + ax + b \pmod{31}$, niin saadaan kongruenssiyhtälöpari:

$$\begin{cases} 3^2 \equiv 12^3 + 12a + b & \pmod{31} \\ 9^2 \equiv 1^3 + a + b & \pmod{31} \end{cases}$$

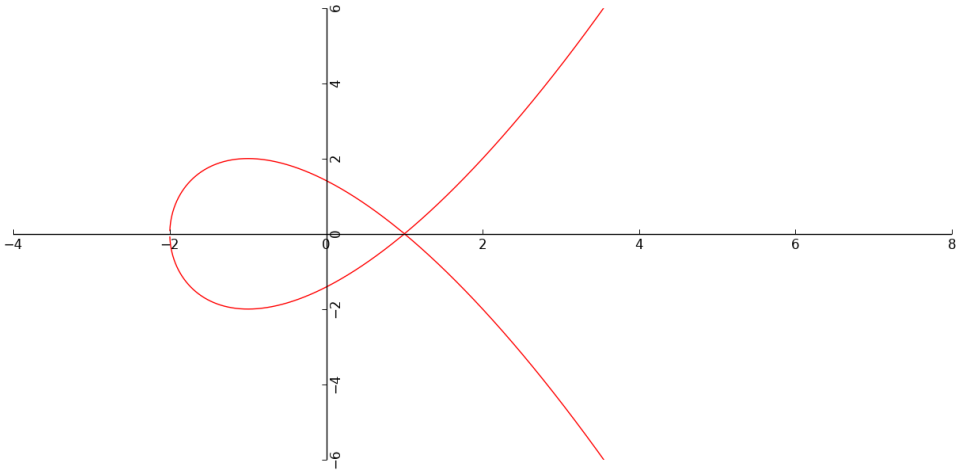
eli

$$\begin{cases} b \equiv -1719 - 12a \equiv 17 - 12a & \pmod{31} \\ b \equiv 80 - a \equiv 18 - a & \pmod{31} \end{cases}$$

Siten $17 - 12a \equiv 18 - a \pmod{31}$ eli $11a \equiv -1 \pmod{31}$. Tästä saadaan $a \equiv 14 \pmod{31}$. Siis voidaan valita $a = 14$. Tällöin $b \equiv 18 - a \equiv 18 - 14 = 4 \pmod{31}$. Kysytty elliptinen käyrä on siis $y^2 = x^3 + 14x + 4 \pmod{31}$. On helppo tarkistaa, että tämä käy.

6. Hahmottele käyrän $y^2 = x^3 - 3x + 2$ kuvaaja reaalilukujen joukossa (hyvin karkea hahmotelma riittää). Totea, että käyrän diskriminantti on nolla, ja päättele kuvaajasta (tai muuten) missä pisteissä ongelmia muodostuisi. (Toisin sanoen, missä pisteissä olisi ongelmia tangentin määrittelyn kanssa?)

Ratkaisu. Kuvaaja näyttää tältä:



Diskriminantti on $-16(4a^3 + 27b^2) = -16(4 \cdot (-3)^3 + 27 \cdot 2^2) = 0$. Ongelma tangentin määrittelyn kanssa tulee pisteessä $(1, 0)$, sillä käyrä leikkaa itsensä tässä pisteessä. Tähän pisteeseen voidaan nimittäin piirtää käyrälle kaksi tangenttia.