KRYPTOGRAFIAN ALKEET

5. LASKUHARJOITUKSET

(1) Piirrä käyrän $y^2 = x^3 - 5x$ kuvaaja modulossa 7 ja hahmottele se 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.
(3) Laske pisteiden $P = (0, 0)$ ja $Q = (-1, 2)$ summa kunnassa $\mathbb{Z}_7$.
(4) Laske $2Q$ käyrällä $y^2 = x^3 - 5x$ sekä reaalilukujen joukossa että kunnassa $\mathbb{Z}_7$, kun $Q = (-1, 2)$.
(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.
(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?)