KRYPTOGRAFIAN ALKEET

5. RÄKNEÖVNINGEN

(1) Rita grafen på kurvan $y^2 = x^3 - 5x$ modulo 7 och skissera grafen i mängden av reella talen.
(2) Uppskatta med hjälp av bilden i uppgift ett vad summan av punkterna $P = (0, 0)$ och $Q = (-1, 2)$ är. Beräkna summan av punkterna i realtalsfallet.
(3) Beräkna summan av punkterna $P = (0, 0)$ och $Q = (-1, 2)$ i kroppen $\mathbb{Z}_7$.
(4) Beräkna $2Q$ på kurvan $y^2 = x^3 - 5x$ både i mängden av reella talen och i kroppen $\mathbb{Z}_7$, då $Q = (-1, 2)$.
(5) Del a och b är alternativa:
   (a) Rita med hjälp av en dator den elliptiska kurvan $y^2 = x^3 + 200x + 192$ i kroppen $\mathbb{Z}_{281}$ och räkna upp dess punkter.
   (b) En elliptisk kurva i kroppen $\mathbb{Z}_{31}$ har punkterna $(12, 3)$ och $(1, 9)$. Finn kurvan.
(6) Skissera grafen för kurvan $y^2 = x^3 - 3x + 2$ i mängden av reella talen (en grov skiss räcker). Konstatera att kurvans diskriminant är noll, och finn med hjälp av grafen (eller på annat vis) de punkter var problem skulle uppstå, dvs. de punkter var vi skulle få problem med definitionen på tangenten.