The electronic health card, summer 2008

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

11. Exercise sheet
Hand in solutions until Monday, 14 July 2008.

Exercise 11.1 (The Size of an Elliptic Curve). (5 points)

In this exercise we will explore how the sizes of elliptic curves over some particular small finite field are distributed.

(i) Write a small program that counts the number of points of all elliptic curves in Weierstraß form over $\mathbb{F}_{11}$. To do so, generate all possible equations of the form $y^2 = x^3+ax+b$ with $a, b \in \mathbb{F}_{11}$ and count for each choice of a and b how many pairs $(x, y) \in \mathbb{F}_{11}^2$ exist that fullfill that equation. Do not forget to count the point at infinity! [3]

(ii) Nicely plot the statistics and compare your results to Hasse's bound $|\#E - q - 1| \leq 2\sqrt{q}$. [2]

Exercise 11.2 (ePrescriptions). (6 points)

Consider the service electronic prescription.

(i) Formulate the life cycle of a prescription. [1]

(ii) Describe the high level view of the necessary commands to be implemented on the card for electronic prescriptions. [2]

(iii) Which security means do you suggest? Do not forget to consider practicability and that the patient shall be able to see his prescriptions even without a doctor (or equivalent) at his side. [3]