Cryptology, homework sheet 6

Due for 2MMC10: 20 October 2016, 10:45
and for Mastermath: 1 December 2016, 10:45 by email to `crypto.course@tue.nl`

Team up in groups of two or three to hand in your homework. We do not have capacity to correct all homeworks individually. Do not email Tanja your homework or put homework in mailboxes.
You may use computer algebra systems such as mathematica, gp, or sage or program in C, Java, or Python. Please submit your code if any) as part of your homework. If you do, make sure that your programs compile and run correctly; my students will not debug your programs. The program should also be humanly readable.

1. Prove that for (x_1, y_1) and (x_2, y_2) on the circle $x^2 + y^2 = 1$ also their sum $(x_1, y_1) + (x_2, y_2) = (x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$ is on the circle.

2. Find all points (x_1, y_1) on the Edwards curve $x^2 + y^2 = 1 - 5x^2y^2$ over $\mathbb{F}_{13}$. Show how you can use symmetries in the curve equation. Do not solve this exercise by brute force on a laptop.

3. Verify that $P = (6, 3)$ and $Q = (3, 7)$ are on the curve $x^2 + y^2 = 1 - 5x^2y^2$ over $\mathbb{F}_{13}$. Compute $R = 2P + Q$.

4. Consider the short Weierstrass equation $y^2 = x^3 + ax + b$ over a field of characteristic not equal to 2 or 3. Show that the curve is not an elliptic curve, i.e. the curve is singular, if and only if $4a^3 + 27b^2 = 0$.