University of Limerick
Dr. Bernd Kreussler

5 November 2015
Exercise Sheet 9

MA 6011 (Cryptographic Mathematics)

Solve Problems 1 and 2 ***before*** *the tutorial on Tuesday, 17 November.*

Problem 1: Let the elliptic curve E be given by $y^2 = x^3 + 13x + 5$ modulo 43.

(i) Verify that $A = (7, 3)$ and $B = (4, 11)$ are $\mathbb{F}_{43}$-points on E.

(ii) Calculate the $\mathbb{F}_{43}$-point $A + B$.

(iii) Calculate the $\mathbb{F}_{43}$-point $3A$.

Problem 2: Complete the table below and use it to find the number of $\mathbb{F}_5$-points on the elliptic curves $y^2 = x^3 + 3x + c$ for $c = 0, 1, 2, 3, 4$.

x	x^3	$3x$	$x^3 + 3x$	$x^3 + 3x + 1$	$x^3 + 3x + 2$	$x^3 + 3x + 3$	$x^3 + 3x + 4$
0	0	0	0	1	2	3	4
1	1						
2	3						
3	2						
4	4						
number of points							

Use sage to solve the following ***before*** *we meet for the lab on Tuesday, 10 November.*

Problem 3: What range of values are possible for the number of $\mathbb{F}_7$-points on an elliptic curve according to Hasse's Theorem? For each of those values find a corresponding elliptic curve.

Problem 4: Calculate the number of $\mathbb{F}_p$-points and the p-defect of the elliptic curve

$$y^2 = x^3 + 17$$

for all prime numbers p satisfying $5 \leq p < 200$ and $p \neq 17$.
Characterise those primes p for which the p-defect is equal to zero.

CHALLENGE: Can you prove a general statement about primes p for which the p-defect of this curve is equal to zero?
HINT: Use Fermat's Little Theorem and think RSA.