University of Limerick
Dr. Bernd Kreussler

29 October 2015
Exercise Sheet 8

MA 6011 (Cryptographic Mathematics)

Solve Problems 1–4 ***before*** *the tutorial on Tuesday, 3 November.*

In Problems 1–4, the elliptic curve E has equation $y^2 = x^3 + 17$.

Problem 1: Verify that each of the following points lies on E.

$A = (-2, 3)$ $B = (-2, -3)$ $C = (-1, 4)$ $D = (-1, -4)$
$F = (2, 5)$ $G = (2, -5)$ $H = (4, 9)$

Problem 2: Determine the following points and verify that they are indeed on E.

(i) $A + C$

(ii) $B + D$

(iii) $C + F$

(iv) $A + G$

(v) $G + H$.

Problem 3: Determine $2C$, $2F$ and $2H$ and verify that they are indeed on E.

Problem 4: Find one point with integer coordinates lying on E other than those seen in Problems 1, 2 and 3.

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

Problem 5: Let E be the elliptic curve $y^2 = x^3 - 3x + 7$.

(i) Verify that $P = (-1, 3)$ is a point on E .

(ii) Determine the multiples kP for $k = 1, 2, \ldots, 20$.

(iii) Calculate $2014P$.