University of Limerick
Dr. Bernd Kreussler

12 November 2015
Exercise Sheet 10

MA 6011 (Cryptographic Mathematics)

Solve Problems 1–4 ***before*** *the tutorial on Tuesday, 17 November.*

Problem 1: Let the Edwards curve E be given by $x^2 + y^2 = 1 + 27x^2y^2$ modulo 53.

(i) Verify that $A = (26, 4)$ and $B = (3, 48)$ are $\mathbb{F}_{53}$-points on E.

(ii) Calculate the $\mathbb{F}_{53}$-point $A + B$.

(iii) Calculate the $\mathbb{F}_{53}$-point $3A$.

Problem 2: If p is a prime number, the set $U_p = \{1, 2, \dots, p-1\}$ is a multiplicative abelian group. Find the order of each element in U_{13}.

Problem 3: Find the order of each $\mathbb{F}_5$-point on the elliptic curve $y^2 = x^3 - 3x^2 + 3x$.

Problem 4: Use the Silver-Pohlig-Hellman algorithm to solve $3^x \equiv 12 \mod 19$.

Use sage to solve the following ***before*** *we meet for the lab on Tuesday, 24 November.*

Problem 5: For each divisor d of 52 find how many elements in the multiplicative abelian group U_{53} have order d.