University of Limerick
Dr. Bernd Kreussler

19 November 2015
Exercise Sheet 11

MA 6011 (Cryptographic Mathematics)

Solve Problems 1–4 ***before*** *the tutorial/lab on Tuesday, 24 November.*

Problem 1: Use Fermat Factorisation to factorise

(i) $n = 4717$

(ii) $n = 17363$

(iii) $n = 29651$

Problem 2: Use Pollard's rho method to factorise $n = 10349$. Use starting value $x_0 = 2$ and iterate the function $f(x) = x^2 + 1$.

Problem 3: Let E be the elliptic curve given by the equation $y^2 = x^3 + x - 1$. The point $P = (1, 1)$ is on E. All calculations will be carried out modulo $n = 77437$. We have chosen $k = 7776000 = 2^8\,3^5\,5^3$ and during our calculation of kP we found that $Q = 2^8 \cdot 3^5 \cdot P = (29373, 8488)$. In order to calculate $5Q$ we found that $4Q = (21666, 35552)$.
Use this information and Lenstra's elliptic curve method to factorise $n = 77437$.

Problem 4: Use Pollard's $p - 1$ method to factorise $n = 10057$. Use $B = 5$ and work with $a = 2, 3, \dots, 20$.