University of Limerick
Dr. Bernd Kreussler

24 September 2015
Exercise Sheet 3

MA 6011 (Cryptographic Mathematics)

Tuesday, 6 October: Problems 1–4 at tutorial.

Problem 1: Find the following residues (smallest positive integer):

(i) $2014^{16} \mod 17$

(ii) $57^{102} \mod 101$

(iii) $2^{600} \mod 199$

Problem 2:

(i) Find $\varphi(60)$, then calculate $7^{50} \mod 60$.

(ii) Find $\varphi(1001)$, then calculate $2^{7927} \mod 1001$.

(iii) Find $\varphi(32)$, then calculate $11^{79} \mod 32$.

Problem 3: Verify that $\varphi(84) = \varphi(12)\varphi(7)$ by finding a one-to-one relationship (bijection) between ordered pairs and coprime residues mod 84.

Problem 4:
Solve the system of congruences

$$\begin{aligned} x &\equiv 1 \mod 7 \\ x &\equiv 3 \mod 11 \\ x &\equiv 5 \mod 13 \end{aligned}$$

The following will be discussed at the lab on Tuesday, 29 September. Try to write a sage program that gives the answer. Do this before we meet for the lab.

Problem 5: Draw up a table of $a^k \mod 11$ for $0 \leq a \leq 10$ and $1 \leq k \leq 12$. Use this table to verify Fermat's little theorem for the prime $p = 11$.

Problem 6:

(i) Determine $5^{322} \mod 323$. Is 323 a prime number?

(ii) Determine $2^{2008} \mod 2009$. Is 2009 a prime number?