University of Limerick
Dr. Bernd Kreussler

17 September 2015
Exercise Sheet 2

MA 6011 (Cryptographic Mathematics)

Tuesday, 22 September: Problems 1–4 and problems from sheet 1 at tutorial.

Problem 1: Use Euclid's Lemma to prove the following result which was stated in the lecture notes.

> Let p be a prime number which is a divisor of the product $a_1a_2a_3\cdots a_n$ of integers. Then p is a divisor of (at least) one of the factors $a_1, a_2, \ldots, a_n$.

Problem 2: Find the prime factorisations of

$$500,\ 501,\ 502,\ 503,\ 504,\ 505,\ 506,\ 507,\ 508,\ 509.$$

Which of the prime numbers less than 23 divide one of these numbers?

Problem 3:

(i) Prove that if $a \equiv b \mod m$ and $c \equiv d \mod m$, then $ac \equiv bd \mod m$.

(ii) Deduce that if $a \equiv b \mod m$, then $a^k \equiv b^k \mod m$ for all $k \geq 1$.

Problem 4: Solve these congruences.

(i) $6\,x \equiv 4 \mod 10$

(ii) $10\,x \equiv 4 \mod 6$

(iii) $56\,x \equiv 100 \mod 236$

(iv) $x^2 \equiv -1 \mod 17$

(v) $x^3 \equiv 1 \mod 7$

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 at the lab.

Problem 5: Apply the sieve of Eratosthenes to find the prime numbers less than 1000. Compare your result with the `sage` list obtained with the command `primes(1000)`.

Problem 6: Find the prime factorisations of $2000, 2001, 2002, \ldots, 2012, 2013, 2014$. Which of the prime numbers less than 45 divide one of these numbers?