University of Limerick
Dr. Bernd Kreussler

8 October 2015
Exercise Sheet 5

MA 6011 (Cryptographic Mathematics)

Solve Problems 1–9 ***before*** *the tutorial on Tuesday, 20 October. You may use sage to do some of the calculations.*

Problem 1: Can pq be a Carmichael number when p and q are odd primes?

Problem 2: Find a positive integer k such that $6k+1$, $12k+1$ and $18k+1$ are prime numbers. Prove that then $(6k+1)(12k+1)(18k+1)$ is a Carmichael number. Use sage to find at least ten such Carmichael numbers.

Problem 3: Use Korselt's criterion to verify that 2465 is a Carmichael number.

Problem 4: For $a = 5, 7, 13$ test if 341 is a Fermat pseudoprime to base a.

Problem 5: Find a Rabin-Miller witness $a > 8$ for $n = 1729$.

Problem 6: Find all integers $1 \leq a < 667$ for which $a^{666} \equiv 1 \mod 667$.

Problem 7: Find all primes $p < 100$ for which 3 is a primitive root modulo p.

Problem 8: Verify that 2 is a primitive root modulo 53 and draw up the corresponding table of indices.

Problem 9: Use Shanks' Baby-step Giant-step algorithm to solve $5^x \equiv 96 \mod 317$.