PMATH 340 Number Theory, Assignment 4 — Due: Mon Apr 8, 11:00 pm

1: (a) Let $n = 493$, $e = 85$ and $c = 261$. Decipher the ciphertext c to recover the original message m that was encrypted using the RSA scheme with the public key (n, e).

(b) Show that if many users choose a small value for their encryption key then the RSA scheme can be weak. To be specific, show that if A sends the same short message m to three individuals B_1, B_2 and B_3 who have public keys (n_i, e_i) with n_1, n_2 and n_3 distinct, and with $e_1 = e_2 = e_3 = 3$, then an eavesdropper E who intercepts the three encrypted messages $c_i = m^{e_i} = m^3 \bmod n_i$ can recover the original message m.

2: (a) Use Fermat's Little Theorem and the Square and Multiply Algorithm to show that 2479 is not prime (without testing each prime $p \leq \sqrt{2479}$ to see if is a factor). You can use a calculator for this problem.

(b) Determine whether 561 is a pseudo-prime, and whether 561 is a strong pseudoprime, for the base 5.

(c) Find (with proof, of course) every prime number p such that $7 \cdot 19 \cdot p$ is a Carmichael number.

3: (a) Let $a \geq 2$ and $m \geq 1$ be integers. Show that if $a^m + 1$ is prime, then a must be even and m must be a power of 2.

(b) Show that the Mersenne number M_{13} is prime and that the Mersenne number M_{23} is composite. You can use a calculator for this problem.

(c) Show that if n is a pseudoprime for the base 2 then so is the Mersenne number $M_n = 2^n - 1$.

4: (a) Show that there are infinitely many primes of the form $12k + 7$ with $k \in \mathbb{Z}$.

(b) Find (with proof, of course) the smallest positive integer k with the property that there exists a prime number p such that the six numbers p, $p + k$, $p + 2k$, $p + 3k$, $p + 4k$ and $p + 5k$ are all prime.