Homework 3

Due: Thursday April 25, 2013

1. For any positive real number r, prove that $x^r = O(e^x)$ as functions of x.

2. Compute the continued fraction expansion of the three numbers $427/67$, $\sqrt{7}$ and $\tan(1)$. (For the latter number, you don't need to prove the result you get is correct, simply do enough computations to be able to guess the pattern (and show how these computations were performed). Of course 1 is in radians).

3. In the continued fraction expansion of $\sqrt{7}$ calculated in the previous problem, let n be any integer such that $a_{n+1} = 2a_0$. Compute the convergent p_n/q_n and show that $x = p_n$, $y = q_n$ gives a solution to Pell's equation $x^2 - 7y^2 = 1$.

4. Let $N = 8633243$. You compute that $2^{8633242} \equiv 8236849 \pmod{N}$. From this information, what can you conclude about the prime factorisation of N?

5. Let a and n be positive integers with $\gcd(a, n) = 1$. The *order* of a modulo n (denoted $\operatorname{ord}_n(a)$) is defined to be the smallest positive integer d such that $a^d \equiv 1 \pmod{n}$.

   Let r be a positive integer. Prove that $a^r \equiv 1 \pmod{n}$ if and only if r is divisible by $\operatorname{ord}_n(a)$. (This is Exercise 20 in Chapter 3 of Trappe & Washington, which gives out hints for the proof).

6. The number n is said to be a *strong pseudoprime* to the base b if it passes the Miller-Rabin test to base $a = b$. Show that 65 is a strong pesudoprime to base 8 and base 18 but not to base 14 (which is the product of 8 and 18 modulo 65).

7. Let n be an odd composite integer which is either a prime power or divisible by an integer which is congruent to 3 modulo 4. Suppose that n is a strong pseudoprime to the bases b_1 and b_2. Prove that n is a strong pseudoprime to the base $b_1 b_2$.