Homework 2

Due: Thursday April 19, 2012

1. Two possible definitions of ISBN numbers are

   (a) Strings $a_1 a_2 \cdots a_{10}$ such that $a_1 + 2a_2 + \cdots + 9a_9 + 10a_{10} \equiv 0 \pmod{11}$,

   (b) Strings $a_1 a_2 \cdots a_{10}$ such that $10a_1 + 9a_2 + \cdots + 2a_9 + a_{10} \equiv 0 \pmod{11}$.

   Prove that these two definitions are equivalent. (ie, a string is an ISBN number under the first definition if and only if it is an ISBN number under the second defition).

2. Show that 0-13-116093-8 is not a valid ISBN number, and find two diferent valid ISBN numbers that each differ from 0-13-116093-8 in exactly one digit. (This shows that although the ISBN scheme can detect a single error, it cannot correct a single error).

3. The ciphertext 75 was obtained using the RSA algorithm with $n = 437$ and $e = 3$. You know that the plaintext is a positive integer less than 10. Determine which integer this is without factoring n.

4. Three RSA users have public keys with modulus N_1, N_2, N_3 (you may assume if you want that these moduli are pairwise coprime) and each use the encryption exponent $e = 3$. Suppose that the same message m $(0 \leq m \leq N_i)$ is sent to each RSA user, and you intercept the three ciphertexts $c_i \equiv m^3 \pmod{N_i}$ for $i = 1, 2, 3$.

   Show that $0 \leq m^3 \leq N_1 N_2 N_3$, and hence that using the Chinese remainder theorem, you can not only calculate the value of $m^3 \pmod{N_1 N_2 N_3}$, but that you actually obtain the exact value of m^3 and hence can read the message m.

5. Find the remainder when 5^{1056} is divided by 7.

6. Find all four solutions to $x^2 \equiv 1 \pmod{187}$.

7. Let p and q be distinct primes. Prove that $\phi(pq) = (p-1)(q-1)$.

8. Using the inequality from the previous problem set

   $$\prod_p p^{\lfloor \log_p(2n) \rfloor} \geq \binom{2n}{n},$$

   prove that there are infinitely many primes. For this you will need a handle on how large the right hand side is. There is an estimate $\binom{2n}{n} \geq 4^n/(2n+1)$ which is obtained as follows: Expand $4^n = (1+1)^{2n}$ using the binomial expansion. There are a total of $2n+1$ terms and the largest is $\binom{2n}{n}$.