MATH 135 F 2012: Assignment 8

Due: 8:30 AM, Wed., 2012 Nov. 14 in the dropboxes outside MC 4066
or in the electronic dropbox for students in the online section

Write your answers in the space provided. If you wish to typeset your solutions, use one of the solution templates posted on the course web site.

Family Name:

First Name:

I.D. Number:

Section:

Mark: (For the marker only.)

If you used any references beyond the course text and lectures (such as other texts, discussions with colleagues or online resources), indicate this information in the space below. If you did not use any aids, state this in the space provided.

---

1. This question is intended to reinforce the mechanics of the RSA scheme. Suppose that in setting up RSA, Alice chooses $p = 71$, $q = 101$ and $e = 13$.

   (a) What is Alice's public key?

   (b) What is Alice's private key?

   (c) Suppose Alice wishes to send Bob the message $M = 2012$. Bob's public key is $(17, 2747)$. What is the cipher text corresponding to the message? Feel free to use a calculator or Maple to help with calculation.

(d) Suppose Alice receives the cipher text 314. What was the original message? Feel free to use a calculator or Maple to help with calculation.

2. Let N, c, m be integers. Suppose $m = m_1 m_2$ where m_1, m_2 are positive integers with $\gcd(m_1, m_2) = 1$.

   (a) A key part in the proof of the RSA algorithm is the following result. Prove this proposition.

   Proposition 1. *The linear congruence*

   $$N \equiv c \pmod{m}$$

   is satisfied if and only if the following system of linear congruences is satisfied

   $$\begin{cases} N \equiv c \pmod{m_1} \\ N \equiv c \pmod{m_2} \end{cases}$$

   (b) Suppose $\gcd(m_1, m_2) > 1$. Then one direction of Proposition 1 is no longer true. Identify this direction, and provide a counterexample.

   (c) Prove that for any integer n,

   $$441n^{43} + 374n^{35} + 285n^{23} \equiv 0 \pmod{55}.$$

3. Given prime numbers p and q where $p > q$, let $n = pq$ and $\phi(n) = (p-1)(q-1)$.

   (a) Prove that
   $$p + q = n - \phi(n) + 1, \qquad p - q = \sqrt{(p+q)^2 - 4n}.$$

   (b) Prove that if $p - q$ is known, then part (a) can be used to factor n.

   (c) Part (b) can be used to factor n when the difference between p and q is not too large, say bounded by a constant k. Describe a method for factoring n when $p - q \leq k$, and use this method to factor $n = 60140021$ given that $p - q \leq 10$.

4. Let f map from the set of country names to the letters of the alphabet be defined by taking as the image of the name of the country the first letter of the name. For example, $f(\text{Canada}) = C$. Prove that f is a bijection or show by counterexample that it is not. You will find the list of countries at `http://en.wikipedia.org/wiki/List_of_sovereign_states` helpful.

5. Let $f : \mathbb{Z}_m \setminus \{[0]\} \to \mathbb{Z}_m \setminus \{[0]\}$ be defined by $f([x]) = [x]^{-1}$. For each of the following, prove that f is a bijection or show by counterexample that it is not.

   (a) $m = 5$

   (b) $m = 6$

6. This question will give you some practice with a mapping that will be used to prove that $|\mathbb{N}\times\mathbb{N}| = |\mathbb{N}|$. Let

$$\mathbb{N} \times \mathbb{N} = \{(a, b) \mid a, b \in \mathbb{N}\}$$

and consider the rule $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by $f((a, b)) = 2^{a-1}(2b - 1)$.

   (a) What are the images of the following elements?
      i. $(1, 1)$
      ii. $(2, 3)$
      iii. $(3, 11)$

   (b) What elements, if any, map onto the following natural numbers?
      i. 15
      ii. 16
      iii. 120

7. Let S be the set of all subsets of $\mathbb{N}$. Let $f : \mathbb{N} \to S$ be defined by

$$f(n) = \{d \in \mathbb{N} : d \mid n\}$$

   (a) What is $f(6)$?

   (b) What is $f(7)$?

   (c) Prove that f is a surjection or show by counterexample that it is not.

   (d) Prove that f is an injection or show by counterexample that it is not.

8. (Modified from *Introduction to Mathematical Proofs* by Charles Roberts Jr. pg. 155) The identity function $f : (0, 1) \to (0, 1)$ defined by $f(x) = x$ is a bijection. Give an example of another bijection $g : (0, 1) \to (0, 1)$ such that $f(x) \neq g(x)$ for all $x \in (0, 1)$. Be sure to show that g is a bijection and that $f(x) \neq g(x)$ for all $x \in (0, 1)$.

9. Consider the following proposition.

   Proposition 2. *If* $\gcd(u, v) = 1$ *and* $m \in \mathbb{N}$*, then there exists an integer solution to* $ux + vy = m$*.*

   Suppose that a student writes the following "proof".

   Proof.

$$ux + vy = 1$$

$$umx + vmy = m$$

   □

   The student is angry that the solution is only given one mark out of four. What should the proof look like?