CS/MATH111 ASSIGNMENT 2

due Thursday, April 28 (8AM)

Individual assignment: Problems 1 and 2.
Group assignment: Problems 1,2 and 3.

Problem 1: Prove that equation

$$p^2 = q - 2$$

has exactly one solution in which p and q are prime. Thus you need to do two things: (i) find a solution where with both p, q prime, and (ii) prove that there are no other solution in prime numbers.

Hint: In part (ii) consider cases, depending on the remainder of q modulo 3.

Note: The grading will take into account not only correctness, but also the clarity and rigor of the presentation.

Problem 2: Alice's RSA public key is $P = (e, n) = (47, 115)$. Bob sends Alice the message by encoding it as follows. First he assigns numbers to characters: blank is 2, comma is 3, period is 4, semicolon is 5, dash is 6, then A is 7, B is 8, ..., Y is 31, and Z is 32. Then he uses RSA to encode each number separately.

Bob's encoded message is:

39	40	102	40	82	40
108	113	96	40	61	65
8	40	100	8	96	99
66	8	82	40	74	40
96	82	66	100	100	8
74	18	82	96	40	68
82	40	39	113	96	40
61	65	8	61	3	8
18	65	65	66	39	66
100	100	113	24	6	8
65	66	39	66	100	100
40	96	40	66	100	64

Decode Bob's message. Notice that you don't have Alice's secret key, so you need to "break" RSA to decrypt Bob's message.

For the solution, you need to provide the following:

- Describe step by step how you arrived at the solution:
  - Show how you determined p, q, $\phi(n)$, and d;
  - Show the calculation that determines the first letter in the message.
- Give Bob's message in plaintext. The message is a quote. Who said it?
- If you wrote a program, attach your code to the hard copy. If you solved it by hand (not recommended), attach your scratch paper with calculations.

Problem 3: (a) Compute $14^{-1} \pmod{19}$ by enumerating multiples of the number and the modulus. Show your work.

(b) Compute $14^{-1} \pmod{19}$ using Fermat's theorem. Show your work.

(c) Find a number $x \in \{1, 2, ..., 40\}$ such that $7x \equiv 11 \pmod{41}$. Show your work. (You need to follow the method covered in class; brute-force checking all values of x will not be accepted.)

Submission. To submit the homework, you need to upload the pdf file into ilearn by 8AM on Thursday, April 28, and turn-in a paper copy in class.