CS/MATH111 ASSIGNMENT 2

Problem 1:
Let $n > 1$ be an integer.
a) Let $m = n^4 + 4^n$. Is m prime or composite? Provide a proof. (You may need to use Sophie Germain's identity for your proof).
b) Let $m = n^3 + 2$. If both, n and $n^2 + 2$, are prime integers, is m prime or composite? Provide a proof.

Problem 2:

Alice's RSA public key is $P = (e, n) = (35, 65)$. Bob sends Alice the message by encoding it as follows. First he assigns numbers to characters: A is 2, B is 3, ..., Z is 27, and blank is 28. Then he uses RSA to encode each number separately.

Bob's encoded message is:

```
11    33    31     7    33     7    52
30    17    11     7    28    24    61
57     7    28    30    24    15    31
7     31    29    30    20    57     7
30    20     7    31    29    11     7
14    61    24    20    30    20    57
 7    33    20    60     7    20    61
31    29    30    20    57     7    19
61    24    15    11     7    19    30
52    52     7    29    33    23    23
11    20     7    31    61     7    26
61     3     7    31    29    11     7
24    11    15    31     7    61    28
 7    31    29    11     7    60    33
26
```

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

For the solution, you need to provide the following:

- (a) Describe step by step how you arrived at the solution.
- (b) Show your work (the computation) for the first three numbers in the message.
- (c) Give Bob's message in plaintext (also, what does it mean and who said it?).
- (d) Show (attach) your code for the remaining numbers. The code can be written in any programming language.

Problem 3:
(a) Compute $13^{-1} \pmod{23}$ by enumerating multiples. Show your work.
(b) Compute $13^{-1} \pmod{23}$ using Fermat's Little Theorem. Show your work.
(c) Compute $11^{-11} \pmod{19}$ using Fermat's Little Theorem. Show your work.
(d) Use Fermat's Little Theorem to compute $7^{1209643} \pmod{11}$. Show your work.

(e) Find an integer x, $0 \leq x \leq 40$, that satisfies $31x + 42 = 4 \pmod{41}$. Show your work. You should not use brute force approach.

(f) Calculate $138^{-1} \pmod{2784}$ using any method of your choice. Show your work.

(g) How many integers have inverses modulo 144? Justify.

(h) Prove, that if a has a multiplicative inverse modulo N, then this inverse is unique (mod N).

Submission. To submit the homework, you need to upload the pdf file into Gradescope (only one copy per group!) and ilearn (individually) .

Reminders. Remember that only LaTeX papers are accepted.