# CS111 w'23 ASSIGNMENT 2

**Problem 1:**

Prove the following statement:
If $p > 5$ and $gcd(p, 20) = 1$, then $(p^2 - 21)(p^2 + 16) \equiv 0 \pmod{20}$.

*Hint:* The product of any $k$ consecutive integers is divisible by $k$.

**Problem 2:**

Alice's RSA public key is $P = (e, n) = (7, 4453)$. Bob sends Alice the message by encoding it as follows. First he assigns numbers to characters: A is 7, B is 8, ..., Z is 32, a blank is 33, quotation marks: 34, a coma: 35, a period: 36, an apostrophe: 37. Then he uses RSA to encode each number separately.

Bob's encoded message is:

```
1400 2218   99 2088 4191   84  843   99 4191 3780  764 4191 2979 2269   99  764
2218 2269 2088  843 3015   99 2970 1443 1655   99 3237 2979   99  447 1443 3237
1032 2382  871  843 1655   99  871 1443   99 4242  843   99 4191 2269   99  843
4191 2269 2979   99  871 1443   99 2382 2269  843   99 4191 2269   99 3237 2979
  99  871  843 3780  843 1032 2088 1443 2962  843 2916   99 3237 2979   99  764
2218 2269 2088   99 2088 4191 2269   99  447 1443 3237  843   99  871 1655 2382
 843   99 4242  843  447 4191 2382 2269  843   99 2218   99  447 4191 2962   99
2962 1443   99 3780 1443 2962 1294  843 1655   99 2970 2218 1294 2382 1655  843
  99 1443 2382  871   99 2088 1443  764   99  871 1443   99 2382 2269  843   99
3237 2979   99  871  843 3780  843 1032 2088 1443 2962  843 2916 1400
```

Decode Bob's message. Notice that you don't have Bob's secret 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: find $p$ and $q$, $\phi(n)$ and $d$.

(b) Show your work for one number in the message: the initial expression the decrypted integer, the character that it is mapped to. You don't need to present the computations.

(c) To decode the remaining numbers, you need to write a program in C++, test it on Codeforces, upload to canvas and append the code to HW 2, Problem 2 solutions.

(d) Give the decoded message (in integers).

(e) Give Bob's message in plaintext (also, what does it mean and who said it).

Your program should :

(i) Take three integers, $e$, $n$ (the public key for RSA), and $m$ (the number of characters in the message) as input to your program. Next, input the ciphertext.

(ii) Test whether the public key is valid. If not, output a single line "Public key is not valid!" and quit the program.

(iv) If the public key is valid, decode the message.

(v) Output $p$ and $q$, $\phi(n)$ and $d$.

(vi) On a new line, output the decoded message in integers.

(vii) On a new line, output the decoded message in English. The characters should be all uppercase. You can assume that the numbers will be assigned to characters according to the mapping above: A is 7, B is 8, ... .

Upload your code to Codeforces to test. There are fifteen (open and hidden) test cases. If you implement everything correctly, codeforces will say you have 15 points. The link on how to register/submit code for the RSA project is here. Your score for the RSA code will be based on the score that you received on Codeforces. If you have any questions, post them on Slack.

**Problem 3:**

(a) Compute $5^{1627}$ (mod 12). Show your work.

(b) Compute $8^{-1}$ (mod 17) by listing the multiples. Show your work.

(c) Compute $8^{-1}$ (mod 17) using Fermat's Little Theorem. Show your work.

(d) Compute $8^{-11}$ (mod 17) using Fermat's Little Theorem. Show your work.

(e) Find an integer $x$, $0 \le x \le 40$, that satisfies the following congruence: $31x + 54 \equiv 16$ (mod 41). Show your work. You should not use brute force approach.

**Academic integrity declaration.** The homework papers must include at the end an academic integrity declaration. This should be a brief paragraph where you state *in your own words* (1) whether you did the homework individually or in collaboration with a partner student (if so, provide the name), and (2) whether you used any external help or resources.

**Submission.** To submit the homework, you need to upload the pdf file to Gradescope and the cpp file on canvas (in Assignments). If you submit with a partner, you need to put two names on the assignment and submit it as a group assignment.

**Reminders.** Remember that only LaTeX papers are accepted.