**Problem 1.** Alice wants to encrypt the number 13 using RSA and send it to Bob.

(a) If Bob's public key $e = 3$, and $N = 1081$, what does Alice send to Bob?

(b) If Bob's private key $d = 675$, show the steps Bob would perform to decrypt the message; does he get 13 as expected?

Note: these numbers are small enough that you shouldn'tneed Sage for the calculations.

**Problem 2.** In order to send text using RSA, it is necessary to perform some type of text-to-number encoding first.

For this question, we'll use a simple 2-digt encoding scheme: $a \to 01, b \to 02, c \to 03, \ldots, z \to 26$
So for example, the text "hello" is encoded as 08 05 12 12 15, or 805,121,215 after removing spaces.

(a) Alice wants to encode the message "hi" so she can send it to Bob. What is the numeric encoding of "hi" using our simple scheme?

(b) Alice wants to send this encoded message to Bob using RSA. Bob's public key $e = 7$, $p = 1003001$, and $q = 1000033$. What does Alice send to Bob?

(c) What algorithm would Bob use to calculate his decryption key $d$?

(d) Bob calculates his decryption key $d$ and gets $d = 716451497143$. Show Bob's work, and decrypt the message from Alice; did you get the encoded message that Alice made in part $(a)$?

Note: If the numbers are too big, try using wolframalpha
Note2: Remember, since the encoding gives each letter 2 digits, you may need to add a leading 0 to complete the decoding.

**Problem 3.** Explain in a few sentences (or equations) why $ed \equiv 1 \ (mod \ (p-1)(q-1))$ and not $ed \equiv 1 \ (mod \ pq)$.

**Problem 4.** Prove that $m$ is prime if and only if $\phi(m) = m - 1$.

Taken from Hoffstein 1.21
Note: $\phi()$ is Euler's Totient function.

**Problem 5.** Compute the following values; show your work:

(a) $\phi(6)$

(b) $\phi(9)$

(c) $\phi(15)$

(d) $\phi(17)$

Taken from Hoffstein 3.4