Instructions: Problems 2 and 5 are to be handed in by next Friday (theoretical ones on Moodle, SAGE exercises via CoCalc).

1. Break the code whose RSA enciphering key is $(N, e) = (536813567, 3602561)$ and decipher the message "BNBPPKZAVQZLBJ", under the assumption that the plaintext consists of 6-letter blocks in the usual 26-letter alphabet (converted to an integer between 0 and $26^6 - 1$ in the usual way) and the ciphertext consists of 7-letter blocks in the same alphabet. *(Hint: you may use a computer to find prime factors of N but may not use an existing factoring function)*

2. This exercise is devoted to the study of Carmichael numbers, which are defined as composite integers n who are Fermat pseudoprimes to every base $b \in (\mathbb{Z}/n\mathbb{Z})^*$.

   (a) Prelude: prove that $(\mathbb{Z}/p^k\mathbb{Z})^*$ is cyclic for $p > 2$ and any $k \geq 1$. What about $(\mathbb{Z}/4\mathbb{Z})^*$ and $(\mathbb{Z}/8\mathbb{Z})^*$? *(Hint: for odd p you may assume you have a generator g of $(\mathbb{Z}/p\mathbb{Z})^*$ and show either g or $(p+1) \cdot g$ generates the larger group as well.)*

   (b) Prove that a Carmichael number cannot be divisible by a perfect square. *(Hint: suppose $p^2|n$, let n' be the product of all other primes dividing n. Use CRT to find a base b congruent to a generator modulo p^2 (existing by (a)) and $\equiv 1 \mod n'$. Show n is then not a pseudoprime to the base b.)*

   (c) Prove that a squarefree number n is a Carmichael number if and only if $p-1|n-1$ for every prime divisor p of n. *(For one direction assume $p - 1 \nmid n - 1$ and find a base b as above using now congruences modulo p and n')*

   (d) Use the two previous results to show that a Carmichael number must be the product of at least 3 primes.

   (e) Check that 561 is a Carmichael number (the smallest!); find the next-smallest.

3. If an integer n is composite, then the Miller–Rabin test has at least a 75% chance of succeeding in proving that n is composite, while it never misidentifies a prime as being composite. Suppose we run the Miller-Rabin test N times and it fails to prove that n is composite. Show that the probability that n is prime is approximately

$$\Pr(\ n \text{ is prime} \mid n \text{ failed Miller-Rabin test } N \text{ times }) = 1 - \frac{\ln(n)}{4^N}.$$

   Hint: you are computing the conditional probability of an event E, knowing an event F occurred, denoted $\Pr(E|F)$. Therefore, use Bayes formula

$$\Pr(E|F) = \frac{\Pr(F|E)\Pr(E)}{\Pr(F|E)\Pr(E) + \Pr(F|E^c)\Pr(E^c)}$$

   where E^c denotes the opposite event of E. You may also use the fact that the probability that a random n is prime is about $1/\ln(n)$.

4. Prove that if you find a base b such that n is a (Fermat) pseudoprime to the base b but b is a Miller-Rabin witness for n, you can quickly find a non-trivial factor of n. Explain how to guard against this when choosing $n = pq$ in RSA.

5. The goal of this exercise is to find a large prime number yourself (without using already implemented primality tests)

   (a) Using SAGE, write a function that performs the Miller-Rabin test.

   (b) Play around to find a range of numbers where you can search for primes in reasonable time. Perform the search, finding a number that you believe to be prime with high probability (BIGGER is better!!).

   (c) Can you prove that the number you found is prime? (you may assume the Generalized Riemann Hypothesis)

6. A *Mersenne prime* is a prime of the form $2^n - 1$.

   (a) Prove that $2^n - 1$ is prime only if n is prime, then give a counterexample to the converse.

   (b) See how many Mersenne primes you can find (at least 8) writing your SAGE code from scratch. (so not using SAGE's own algorithms to test primality but yours, though you may reuse code from previous homework problems). Compare with `https://www.mersenne.org/primes/`. Maybe you even want to join the GIMPS?