Week 04, problems.

Modular Exponentiation, Fermat Test, RSA.

1. What is the remainder when 2^{51} is divided by 61? Use an appropriate algorithm done in class to find it.

2. Decide whether the following numbers are Fermat liars, Fermat witnesses, or neither for 15. (To solve this, you may use a calculator and the appropriate algorithms you have learned.)
   a) 2 b) 3 c) 11

3. In the two parts below, you are given two primes p and q and a value e for RSA. Determine if e is suitable, and if yes, find a corresponding d.
   a) $p = 7, q = 11, e = 6$ b) $p = 11, q = 13, e = 7$

4. For $p = 7, q = 13, e = 5, m = 5$, encrypt the message m using RSA with modulus $n = pq$. Find the decryption exponent and verify that you can decode the message.

5. With the encoding function $C : x \mapsto x^{43} \pmod{91}$, we can encode any number from $0, 1, ...90$.
   a) What is the value of $y = C(20)$?
   b) Determine the decoding function $D(y)$ and apply it to the y obtained in the previous part to check the correctness of your decoding function.

---

6. What is the remainder when 3^{86} is divided by 79? Use modular exponentiation algorithm to determine this.

7. Decide whether the following numbers are Fermat liars, Fermat witnesses, or neither for 33. (To solve this, you may use a calculator and the appropriate algorithms you have learned.)
   a) 2 b) 3 c) 23

8. For $p = 3, q = 19, e = 7, m = 5$, encrypt the message m using RSA with modulus $n = pq$. Find the decryption exponent and verify that you can decode the message.

9. A general tells his two lieutenants (labeled a and b) to move m tanks into position for attack. He has encrypted this message using RSA. Decode the message and find the number of tanks assigned to each position.
   a) $p = 3, q = 11, e = 3, c = 7$ b) $p = 5, q = 11, e = 3, c = 9$

---

10. What is the remainder when 5^{300} is divided by 623? Use modular exponentiation algorithm to determine this.

11. Decide whether the following numbers are Fermat liars, Fermat witnesses, or neither for 165. (To solve this, use may use a calculator and the appropriate algorithms you have learned.)
    a) 13 b) 23 c) 33

12. Romeo sends Juliet the hour at which they will meet. He uses RSA with $p = 3, q = 17, e = 5$ The ciphertext is $c = 3$. When will they meet?

13. – What shall we have for lunch?
    – Well, let's say...
    – Be careful, the enemy is listening in on our conversation! Use the encoding function $C : x \to x^{11} \pmod{51}$ to replace the letters of the English alphabet with the numbers 1, 2, ... , 26 in order!
    – You mean...
    – Don't be confused! A = 1, B = 2, C = 3, and so on, finally Z = 26. Don't use accents and don't worry that the other numbers up to 50 have no meaning. So what should we have for lunch?
    – 2, 1, 4.
    Let's determine the decoding function D corresponding to C and use it to figure out what they're having for lunch.

14. * (MT'18) Let n be a positive integer divisible by 8 but not by 3. Show that 3 is a Fermat witness for n.

15. * Show that $561 (= 3 \cdot 11 \cdot 17)$ is a Carmichael number.

Final Answers

1. 28
2. a) Witness, b) Neither, c) Liar
3. no, yes
4. $c = 31, d = 29$
5. 6, $x^{67} \pmod{91}$
6. 4
7. a) Witness, b) Neither, c) Liar
8. $c = 35, d = 31$
9. 28, 4
10. 512
11. a) Witness, b) Liar, c) Neither
12. 12
13. HAM
14.
15.