Name: ______________________________

Math/CS 467, Midterm 1
Fall 2020, John Lesieutre

- Write your exam on a separate sheet of paper and submit on Gradescope.
- You may consult the textbook, your notes, my slides, and the homework solutions during the exam. However, you may not consult other references on the internet.
- No calculators or other aids are allowed.
- Justifications or proofs are required for all problems except where indicated otherwise.
- If you aren't sure how to do a problem, don't leave it blank! I will give you a point or two if you define some of the terms appearing in the problem.
- If you need more space, continue on the back of the page. Mark your work clearly.
- You have 50 minutes to complete the exam.
- Good luck!

Problem 1. Alice is sending a message to Bob using the RSA algorithm. You are a third party who is trying to intercept the message. You saw Bob publish his public key, with numbers $n = 55$ and $e = 7$. You also intercepted the encrypted message, $E = 17$.

a) Bob was sloppy and chose a value of n that is easy to factor. Find the factorization of n and use it to compute $\phi(n)$. (You don't need to use an "official" factorization algorithm.)

b) Now that you know e and $\phi(n)$, you can compute the decryption key d. What is it?

c) Now you have all the information you need to determine the unencrypted message M. What computation would you make to determine this number? (You do not need to actually compute it, but state clearly what needs computed.)

Problem 2. Consider the number 3^n, where n is a positive integer.

a) Write down the factors of 3^n, and compute their sum.

b) Prove that 3^n is not a perfect number.

Problem 3. Suppose you want to test whether $n = 35$ a prime number. You might check whether it is a base-2 pseudoprime. (Yes, I know $n = 35$ is obviously not prime. Play along with me here; I'm using a small number to make your calculations easier.)

a) Define what it means for a number n to be a base-2 pseudoprime. Is every odd prime a base-2 pseudoprime? Why?

b) Is $n = 35$ a base-2 pseudoprime? Make the required computation, and show your work. You may find it helpful to consult the table of squares modulo 35 on the next page.

Problem 4. Suppose you want to find a number a satisfying

$$\begin{aligned} a &\equiv 2 \pmod{7} \\ a &\equiv 0 \pmod{5}. \end{aligned}$$

a) What theorem guarantees that there is a solution to this problem? What hypotheses do you need to check to be sure you can apply the theorem?

b) Find *two* different a that are solutions to these congruences. You can use an algorithm of your choice or simply guess and check, but make sure you find two solutions.

Problem 5. Suppose that $a \equiv b \pmod{n}$ and $x \equiv y \pmod{n}$. Prove that $a + x \equiv b + y \pmod{n}$.

n	0	1	2	3	4	5	6	7	8	9
$n^2 \pmod{35}$	0	1	4	9	16	25	1	14	29	11

n	10	11	12	13	14	15	16	17	18	19
$n^2 \pmod{35}$	30	16	4	29	21	15	11	9	9	11

n	20	21	22	23	24	25	26	27	28	29
$n^2 \pmod{35}$	15	21	29	4	16	30	11	29	14	1

n	30	31	32	33	34	35	36	37	38	39
$n^2 \pmod{35}$	25	16	9	4	1	0	1	4	9	16