

Justify all responses with clear explanations and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly and submit via Gradescope, making sure to select page submissions for each problem. **Use of generative AI in any manner is not allowed on this or any other course assignments.**

Part I: No justifications are required for these problems. Answers will be graded on correctness.

1. Two of the following six integers are prime and the other four are composite:

$$\begin{aligned} N_1 &= 147451228887363586625323456966525905720989842312760509775958662775459536677624741 \\ N_2 &= 181724486732607374235034401344439931270145141565372874381350646276632766328969281 \\ N_3 &= 258424126740178352128100370736889906817607518086806632752038758788555704304604649 \\ N_4 &= 324234657928347051123113232023409710234012389751239847120398471917665655581200339 \\ N_5 &= 408869971164328247524265450583823930434406844303142816841351879439544818685702841 \\ N_6 &= 542408184634943257672698834917404611542248228873337459368210624910406937582942097 \end{aligned}$$

- (a) Try the Fermat test with $a = 2, 3, 5$ for each of these integers. (Stop if you find the integer is composite.)
 - (b) Try the Miller-Rabin test with $a = 2, 3, 5$ for each of the integers not already identified as composite in part (a). (Stop if you find the integer is composite.)
 - (c) Your results from parts (a)-(b) should have identified the four composite numbers. Why don't the results prove that the remaining two integers are actually prime?
-

2. Factor the given integers using the stated procedure, making sure to give enough detail to show that you did actually use that method (just giving the factorization is not sufficient!):

- (a) $N = 1084055561$ by looking for a Fermat factorization.
 - (b) $N = 5686741440097$ by looking for a Fermat factorization.
 - (c) $N = 1032899106233$ by using Pollard's $(p-1)$ -algorithm with $a = 2$.
 - (d) $N = 12038459$ by using Pollard's $(p-1)$ -algorithm with $a = 2$.
 - (e) $N = 1626641013131$ by using Pollard's ρ -algorithm with $a = 2$ and $p(x) = x^2 + 1$.
 - (f) $N = 12038459$ by using Pollard's ρ -algorithm with $a = 2$ and $p(x) = x^2 + 1$.
-

3. Generate (however you like) three 10-digit, three 20-digit, three 30-digit, and three 40-digit numbers: one number should be prime, another should be a product of two primes of roughly equal sizes, and the third should be a product of three primes of roughly equal sizes.

- (a) List the numbers you generated and briefly mention how you generated them.
 - (b) Use the Fermat test (with three residues $a = 2, 3, 5$) and the Miller-Rabin test (with three residues $a = 2, 3, 5$) to test the primality of your integers. How effective are the tests?
 - (c) Do the primality testing algorithms take noticeably longer for the larger numbers than the small ones? Briefly explain.
 - (d) Factor the composite numbers using the Pollard $(p-1)$ - and ρ -algorithms, stopping after a maximum of 1,000,000 steps. List the number of steps each algorithm takes to find a factor.
 - (e) Do the algorithms take more steps for the larger numbers than the smaller ones? Briefly explain.
 - (f) Is there a difference between the number of steps for products of two versus three primes? Briefly explain.
-

4. Consider the Rabin cryptosystem with key $N = 1359692821 = 32359 \cdot 42019$.
- Encode the plaintext $m = 117285016$.
 - Find the four decodings of the ciphertext $c = 823845737$.
-
5. Consider the RSA cryptosystem with key $N = 1085444233 = 31907 \cdot 34019$ and encryption exponent $e = 3$.
- Encrypt the plaintext $m = 277891194$.
 - Find a decryption exponent d .
 - Decrypt the ciphertext $c = 878460400$.
-
6. As proven on homework 2, the only possible primes of the form $a^n - 1$ are the Mersenne numbers $2^p - 1$ where p is a prime. The goal of this problem is to study the prime factorizations of Mersenne numbers.
- Apply the Miller-Rabin test with $a = 2, 3, 5$ on $2^p - 1$ for $p = 11, 13, 17, 19, 23, 29$. You should find that three values are composite: why can you not conclude that the other three values are necessarily prime?
 - Use Pollard's ρ -algorithm with $a = 3$ and polynomial $p(x) = x^2 + 1$ to find the factorizations of the three values $2^p - 1$ you identified as composite in part (a). (Note that the largest one has three prime factors; make sure to find all three by extending the computation past where the first prime factor is found.) How many steps are required to find the factorizations?
-

Part II: Solve the following problems. Justify all answers with rigorous, clear explanations.

7. For all of the factorizations in problem 6, notice that all of the prime factors of $2^p - 1$ are congruent to 1 modulo p . The goal is now to prove this fact, which was first established by Euler. Let p be a prime.
- Suppose that q is a prime that divides $2^p - 1$. Show that the order of 2 modulo q must equal p .
 - Suppose that q is a prime that divides $2^p - 1$. Show that $q \equiv 1 \pmod{p}$.
-
8. Recall that the Lucas primality criterion says that if $a^{m-1} \equiv 1 \pmod{m}$ and $a^{(m-1)/p} \not\equiv 1 \pmod{m}$ for any prime p dividing $m - 1$, then m is prime.
- Use the Lucas primality criterion to show that 1013 is prime, and then establish that 2027 is prime. [Hint: Try $a = 7$ for both.]
 - Use the Lucas primality criterion with $a = 10$ to show that the integer
- $$N = 843156784620274963828079044664499378320177127026840734436833335222593049312927235387489615873$$
- is prime. (If writing by hand, you can just give the first three and last three digits of any large values.)
-