E. Dummit's Math 3527 $\sim$ Number Theory I, Spring 2022 $\sim$ Homework 7, due Fri Mar 25th.

Justify all responses with clear explanations and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly, and clearly identify all problem numbers. Submit scans of your responses via Canvas.

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

1. Eve wants to decipher the ciphertext

$$c = 0992513377540302316114576543616813255831242452697595188311435749125935492869456 6$$

that Alice sent Bob using Bob's RSA key

$$\begin{aligned} N &= 2572184675045399285792021115140418577397380917010975678897958759310601038219880 9 \\ e &= 257. \end{aligned}$$

Eve manages to sneak in and use Bob's decryption computer: she first asks it to decode the message c, but Bob has programmed his computer to remember all of the ciphertexts it has decoded and not allow them to be decoded again, so Eve's first attempt fails. Eve then asks the computer to decipher the message

$$2^e c = 2313495026839688354233041616094754338525390980086277702853335472601541706315212 3$$

and it returns the response

$$w = 0228024828403408002222482608080638282008083008420828101048284034042824304038083 4.$$

From the result, Eve is able to find Alice's original plaintext m that was encoded in the standard way ($\mathbf{a} = 00$, $\mathbf{b} = 01$, ... , $\mathbf{z} = 25$): how did she do this, and what was Alice's message? [Hint: What is the decryption of $2^e c$?]

---

2. Factor the given integers using the stated procedure (make sure to give enough detail so the computations can be followed):

(a) $N = 1\,084\,055\,561$ by looking for a Fermat factorization.

(b) $N = 5\,686\,741\,440\,097$ by looking for a Fermat factorization.

(c) $N = 1\,032\,899\,106\,233$ by using Pollard's $(p-1)$-algorithm with $a = 2$.

(d) $N = 12\,038\,459$ by using Pollard's $(p-1)$-algorithm with $a = 2$.

(e) $N = 1\,626\,641\,013\,131$ by using Pollard's ρ-algorithm with $a = 2$ and $p(x) = x^2 + 1$.

(f) $N = 12\,038\,459$ by using Pollard's ρ-algorithm with $a = 2$ and $p(x) = x^2 + 1$.

---

3. 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 for each of these integers. (Stop after you find the integer is composite, or after 3 tests.)

(b) Try the Miller-Rabin test for each of the integers remaining after part (a). (Stop after you find the integer is composite, or after 3 tests.)

(c) Your results from parts (a)-(b) should have identified the four composite numbers. Why can't either of these tests prove that the remaining two integers are actually prime?

---

4. For each element in each ring $\mathbb{Z}[\sqrt{D}]$, determine (i) whether it is a unit and if so find its multiplicative inverse, and (ii) whether it is irreducible and if not find a nontrivial factorization.

   (a) The elements $-i$, $3+2i$, $1+i$, and $1+5i$ in $\mathbb{Z}[i]$.

   (b) The elements $1+2\sqrt{5}$, $9+4\sqrt{5}$, and $5+\sqrt{5}$ in $\mathbb{Z}[\sqrt{5}]$.

---

5. 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.

   (a) 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?

   (b) 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 identitied 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.

6. For all of the factorizations in problem 5, 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.

   (a) Suppose that q is a prime that divides $2^p - 1$. Show that the order of 2 modulo q must equal p.

   (b) Suppose that q is a prime that divides $2^p - 1$. Show that $q \equiv 1 \pmod{p}$.

---

7. As we have discussed, the Fermat test can only establish that a particular integer is composite, and cannot be used to establish primality. The goal of this problem is to give a refinement, due to Lucas, that can establish primality.

   (a) Suppose m is a positive integer such that there exists an element of order $m - 1$ modulo m. Show that m must be prime.

   (b) Suppose that a and m are positive integers such that $a^{m-1} \equiv 1 \pmod{m}$ but $a^{(m-1)/p} \not\equiv 1 \pmod{m}$ for any prime p dividing $m - 1$. Show that m must be prime.

   The test from part (b) is called the Lucas primality criterion.

   (c) Use the Lucas primality criterion to show that 1013 is prime, and then establish that 2027 is prime. [Hint: Try $a = 7$ for both.]

   (d) Use the Lucas primality criterion with $a = 10$ to show that the integer

   $$N = 843156784620274963828079044664499378320177127026840734436833335222593049312927235387489615873$$

   is prime. (You don't need to write all the results of the modular exponentiations, but just give the first four and last four digits.)
