E. Dummit's Math 3527 ~ Number Theory 1, Spring 2026 ~ Homework 6, due Fri Feb 27th.

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. Eve steals the computer Bob uses to decode messages sent via Rabin encryption. Eve asks the computer to decode the message m^2, where

   $m = 28200654831026650052159579610373580392331220193408318812070409609096292171064290226624500 1$

   and it returns the value

   $w = 16917164509200657824130079912354280309046048566647167876214255454452624124841810165988181 5.$

   Given that Bob's public key is

   $N = 34042444975818554269594748583794531195587594224028027379693238380151635225598207955610628 7,$

   find the two prime factors of N. (If writing by hand, you can just give the first six and last six digits of each.)

---

2. Eve intercepts a 25-character text message with standard encoding ($\mathbf{a} = 00$, $\mathbf{b} = 01$, ... , $\mathbf{z} = 25$) that was encrypted using RSA. Decrypt the message text, given that

   $$\begin{aligned} N &= 513005942752265818136884766599492475562150098362 33 \\ e &= 65537 \\ c &= 425322312108240482509267912832007102477491429539 27. \end{aligned}$$

---

3. Alice sends an identical message with standard encoding ($\mathbf{a} = 00$, $\mathbf{b} = 01$, ... , $\mathbf{z} = 25$) via RSA to each of Bob, Carol, and Darnarius. Each of Bob's, Carol's, and Darnarius's RSA public keys use $e = 3$, and their values of N are, respectively,

   $$\begin{aligned} N_B &= 4970340797887213576836915095173719460384166305298693824751115712679463592127 7619 \\ N_C &= 4839458578512675276009822294243375451877250657448206807998793403498121573045329 3 \\ N_D &= 3704846658184242194508153717209872601307067128009564327936140726043439518675226 7. \end{aligned}$$

   Eve intercepts the three ciphertexts

   $$\begin{aligned} c_B &= 0590536438546628629558625102523766893847219085513235896695772896432360663440025 1 \\ c_C &= 2113822048696114644620661748281185056162976763899408220111197885267660508608180 7 \\ c_D &= 2715712547798440487943101978028812731948382502954384876728073866268308301493921 8. \end{aligned}$$

   Determine Alice's original message.

---

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

   $$\begin{aligned} N_1 &= 1474512288873635866253234569665259057209898423127605097759586627754595366776247 41 \\ N_2 &= 1817244867326073742350344013444399312701451415653728743813506462766327663289692 81 \\ N_3 &= 2584241267401783521281003707368899068176075180868066327520387587885557043046046 49 \\ N_4 &= 3242346579283470511231132320234097102340123897512398471203984719176656555811200 339 \\ N_5 &= 4088699711643282475242654505838239304344068443031428168413518794395448186857028 41 \\ N_6 &= 5424081846349432576726988349174046115422482288733374593682106249104069375829420 97 \end{aligned}$$

   (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?

---

5. Peggy and Victor are performing a Rabin zero-knowledge protocol to prove that Peggy knows s, where

$$\begin{aligned} N &= 488419441734583556321985415212612123740359939381088965700730231638206554681394177 \\ s^2 \pmod N &= 364578471930898294925524638136447727960007605573204140075455802888652544203808336. \end{aligned}$$

Peggy and Victor perform four rounds. Peggy sends Victor

$$\begin{aligned} u_1^2 &= 419987940537002829673554859623446087647247049378701209589622515994832674140645748 \\ u_2^2 &= 270893145623915223448342423282687683714245193752972238573050395604210321017938 02 \\ u_3^2 &= 001204179001250513038323769136188667129468312291612708387897338022926559640599640 \\ u_4^2 &= 295360259330799676568102779994887111797263481168605647699269117672956353312755331 \end{aligned}$$

and Victor asks for the values u_1, su_2, su_3, su_4. Peggy responds with

$$\begin{aligned} u_1 &= 368836285783665928691160226566669484193845816214794656578305054442600293140251910 \\ su_2 &= 061162076090849776429311938634702834494489117638106960807555056103441302535633013 \\ su_3 &= 304092941078945109049230333889649788448145691132625713366641946452437843830720793 \\ su_4 &= 174908257541270590422202403049766598633440061550219493518183063157021792026188460 \end{aligned}$$

Does Peggy pass each test? What is the probability that Eve could pass each test if she didn't know s?

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

6. Bob and his twin brother Rob share the same 4096-bit RSA modulus N, but use different encryption exponents: Bob uses $e_B = 3$ while Rob uses $e_R = 17$. Alice sends the same plaintext message m to Bob and Rob, encoded using their respective keys, so the ciphertexts are $c_B \equiv m^3 \pmod N$ and $c_R \equiv m^{17} \pmod N$. Explain how, if Eve has both ciphertexts c_B and c_R, she can quickly find the original message m without having to factor N.

---

7. Eve wants to decipher the ciphertext c that Alice sent Bob using Bob's RSA key (N, e) so she sneaks in to use Bob's decryption computer. Luckily, Bob has programmed his computer to remember all of the ciphertexts it has decoded and not allow them to be decoded again, so Eve cannot ask it to decipher the message c. Instead, she asks the computer to decipher the message $2^e c$, yielding the deciphered message w. She can use w to find Alice's original plaintext m very quickly: how?

---

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.

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

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

   $$N = 84315678462027496382807904466449937832017712702684073443683333522259304931292723538748961587 3$$

   is prime. (If writing by hand, you can just give the first three and last three digits of any large values.)

---

9. In our discussion of RSA, Bob computes the decryption exponent d as the inverse of e modulo $\varphi(N)$. The goal of this problem is to show that Bob's choice is not always the smallest, as there are always several different possible decryption exponents modulo $\varphi(N)$. (We say k is a decryption exponent for e modulo N if $m^{ek} \equiv m \pmod N$ for every message m.)

   (a) Show that any integer k satisfying $k \equiv d \pmod{p-1}$ and $k \equiv d \pmod{q-1}$ is a decryption exponent. [Hint: Work mod p and mod q separately.]

   (b) Show that any decryption exponent k must satisfy $k \equiv d \pmod{p-1}$ and $k \equiv d \pmod{q-1}$. [Hint: Take m to be a primitive root mod p; you may assume one exists.]

   (c) For $N = 45737 \cdot 54377$ and $e = 3$, Bob's method gives $d = 1657960491$, but this turns out to be the third-largest of 8 possible decryption exponents. Find the smallest one.

   Remark: In general, if $\gcd(p-1, q-1) = r$, using (a) and (b) one can show that there will be r different decryption exponents modulo $\varphi(N)$.
