E. Dummit's Math 3527 ~ Number Theory 1, Spring 2026 ~ Homework 6 Solutions

---

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

   $w = 16917164509200657824130079912354280309046048566647167876214255454452624124841810165988 1815.$

   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.)

   - We implement the chosen-ciphertext attack on Rabin encryption as detailed in class. Since $m^2 \equiv w^2 \pmod N$ by the decryption procedure, and $m \neq \pm w \pmod N$, by the Chinese Remainder Theorem we see that $w + m$ is divisible by exactly one of p and q and so $\gcd(w + m, N)$ will be one of the prime factors of N.
   - Using the Euclidean algorithm to compute the gcds, we obtain

     $$\begin{aligned} \gcd(w+m,N) &= \boxed{637257451356456445706273132863754472582919783} \\ \gcd(w-m,N) &= \boxed{534202384034212978696571376336523449084183289} \end{aligned}$$

     and we can easily verify that their product is the given integer N.

---

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

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

   - In order to decrypt the message we first need to factor the modulus. On my 15-year-old desktop PC, FactorInteger takes approximately 6131 milliseconds to compute the two prime factors as

     $$\begin{aligned} p &= 781775277254987109446814 1 \\ q &= 656206403141272071973441 3. \end{aligned}$$

   - Then $\varphi(N) = (p-1)(q-1) = 513005942752265818136884622801324435936231956336 80.$
   - Next we solve $de \equiv 1 \pmod{\varphi(N)}$. PowerMod / the Euclidean algorithm gives

     $$d = 217908348480058224290013185369230658217385983497 93.$$

   - We can now compute $m \equiv c^d \pmod N$: PowerMod gives

     $$m = 11\,20\,23\,21\,04\,17\,08\,19\,00\,18\,21\,08\,17\,19\,20\,18\,06\,14\,07\,20\,18\,10\,08\,04\,18$$

     which converts into text as $\boxed{\textbf{luxveritasvirtusgohuskies}}$.

---

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.

- We implement Hastad's attack, as detailed in class. The message $x = m^3$ is a solution to the simultaneous congruences $x \equiv c_B \pmod{N_B}$, $x \equiv c_C \pmod{N_C}$, $x \equiv c_C \pmod{N_D}$, and because $m < N_B$, $m < N_C$, $m < N_D$ we have $0 \le m^3 < N_B N_C N_D$ and so the integer solution x to that congruence will actually be equal to m^3 as an integer. By extracting the cube root we then immediately obtain m.
- Solving the congruence using the Mathematica command ChineseRemainder produces the solution

$$\begin{aligned} x = {} & 6935528309374740601405992328601342832140805126478403730309656170009256570064132463681960432373124368490069307383682174848604888723414421147475721220223414093667 \\ & 9642654380808996844529094839349441230327813387801618659543852000162642480576 64 \end{aligned}$$

- Upon extracting the cube root, we obtain Alice's original message

$m = 19\,07\,04\,02\,07\,08\,13\,04\,18\,04\,17\,04\,12\,00\,08\,13\,03\,04\,17\,19\,07\,04\,14\,17\,04\,12\,08\,18\,19\,17\,20\,11\,24\,00\,22\,04\,18\,14\,12\,04$

which as text reads **thechineseremaindertheoremistrulyawesome**.

---

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

$$\begin{aligned} N_1 &= 1474512288873635866253234569665259057209898423127605097759586627754595366776247 41 \\ N_2 &= 1817244867326073742350344013444399312701451415653728743813506462766327663287692 81 \\ N_3 &= 2584241267401783521281003707368899068176075180868066327520387587885555704304604649 \\ N_4 &= 3242346579283470511231132320234097102340123897512398471203984719176656555812003 39 \\ N_5 &= 4088699711643282475242654505838239304344068443031428168413518794395448186857028 41 \\ N_6 &= 5424081846349432576726988349174046115422482288733374593682106249104069375829420 97 \end{aligned}$$

(a) Try the Fermat test with $a = 2, 3, 5$ for each of these integers. (Stop if you find the integer is composite.)

- We compute 2^n, 3^n, and 5^n modulo n for each integer using successive squaring / PowerMod.
- Mod N_1, we get

$$2^n \equiv 8831653594437366449105278288173490547287024673330174195125451834781126651394610 5.$$

The test shows N_1 is composite.

- Mod N_2, we get $2^n \equiv 2$, $3^n \equiv 3$, and

$$5^n \equiv 1817244867326073742350344013444399312699544981879727625387899750142065017155177 46.$$

The test shows N_2 is composite.

- Mod N_3, N_4, N_5, N_6 we get $2^n \equiv 2$, $3^n \equiv 3$, and $5^n \equiv 5$. The test fails for each.

(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.)

- For $n = N_3$ we have $n - 1 = 2^3 d$ where d is odd, so with $j = (n-1)/2^3$ we need to compute a^j, a^{2j}, a^{4j}, a^{8j} mod N_3. With $a = 2$ we obtain

$$\begin{aligned} a^j &\equiv 565099586762790003930515910573623334627549883675608926258504222425788589852750 90 \\ a^{2j} &\equiv 258424126740178352128100370736889906817607518086806632752038758788555704304604648 \\ a^{4j} &\equiv 1 \\ a^{8j} &\equiv 1 \end{aligned}$$

  so since we have an entry of 1 preceded by an entry not ± 1, $\boxed{N_3 \text{ is composite}}$.

- For $n = N_4$ we have $n - 1 = 2d$ where d is odd, so with $j = (n-1)/2$ we need to compute a^j, a^{2j} mod N_3. With $a = 2$ and $a = 3$ we get $a^j \equiv -1$, $a^{2j} \equiv 1$ while with $a = 5$ we get $a^j \equiv 1$, $a^{2j} \equiv 1$, so the $\boxed{\text{test fails}}$.

- For $n = N_5$ we have $n - 1 = 2^3 d$ where d is odd, so with $j = (n-1)/2^3$ we need to compute a^j, a^{2j}, a^{4j}, a^{8j} mod N_3. With $a = 2$ we obtain

$$\begin{aligned} a^j &\equiv 725620373542133587695394596601158435910872362023957672292154921187568081344861 42 \\ a^{2j} &\equiv 400405977139606615533710294266568900454446833681617168 9 \\ a^{4j} &\equiv 1 \\ a^{8j} &\equiv 1 \end{aligned}$$

  so since we have an entry of 1 preceded by an entry not ± 1, $\boxed{N_5 \text{ is composite}}$.

- For $n = N_6$ we have $n - 1 = 2^4 d$ where d is odd, so with $j = (n-1)/2$ we need to compute a^j, a^{2j}, a^{4j}, a^{8j}, a^{16j} mod N_3.
  With $a = 2$ we obtain

$$\begin{aligned} a^j &\equiv 4960756402679058627690363921033767150779475286241902096016833396668842370394099 47 \\ a^{2j} &\equiv 2534565237620067956931510579653135715176837921559470430208687959903465362193030 47 \\ a^{4j} &\equiv -1 \\ a^{8j} &\equiv 1 \\ a^{16j} &\equiv 1 \end{aligned}$$

  With $a = 3$ we obtain

$$\begin{aligned} a^j &\equiv 4596399502983138677135003056792351759730840281669809255469942260154416489232573 74 \\ a^{2j} &\equiv 3399682689124613880063576451474563945857845494509913377591158157843280400899148 46 \\ a^{4j} &\equiv 2889516608729364619795477769520910400245644367173904163473418289200604013636390 50 \\ a^{8j} &\equiv -1 \\ a^{16j} &\equiv 1 \end{aligned}$$

  With $a = 5$ we obtain

$$\begin{aligned} a^j &\equiv 8276823433662938995919852923816943556916420070635653382121639889496528865968 4723 \\ a^{2j} &\equiv 3399682689124613880063576451474563945857845494509913377591158157843280400899148 46 \\ a^{4j} &\equiv 2889516608729364619795477769520910400245644367173904163473418289200604013636390 50 \\ a^{8j} &\equiv -1 \\ a^{16j} &\equiv 1 \end{aligned}$$

  so the $\boxed{\text{test fails}}$.

(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?

- A single application of the Fermat test or the Miller-Rabin test only has the outcomes "n is composite" or "the test is inconclusive": the tests do not say anything in the inconclusive case.

---

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

$$\begin{aligned} u_1^2 &= 419987940537002829673554859623446087647247049378701209589622515994832674140645748 \\ u_2^2 &= 270893145623915322344834242328268768371424519375297223857305039560421032101793802 \\ u_3^2 &= 001204179001250513038323769136188667129468312291612708387897338022926559640599640 \\ u_4^2 &= 295360259330799676568102779994887111797263481168605647699269117672956353312755331 \end{aligned}$$

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?

- Victor simply squares the four values Peggy sent and compares them to the values u_1^2, $s^2u_2^2$, $s^2u_3^2$, and $s^2u_4^2$ evaluated using Peggy's values sent earlier and her public value of s^2.
- Peggy passes rounds 1, 2, and 4 but fails round 3. Explicitly:

$$\begin{aligned} u_1^2 &= 419987940537002829673554859623446087647247049378701209589622515994832674140645748 \\ s^2u_2^2 &= 401461292131569257221239787491164195324644297834820576347826417589549169132643609 \\ s^2u_4^2 &= 179297705882522841343236616001694918781540172739916440334810759330765859061956611 \end{aligned}$$

but

$$\begin{aligned} (su_3)^2 &= 057656109603190227871255310437900913429411389170915685834139712222303307502793574 \\ s^2u_3^2 &= 013092315619048278946259742118943701671041113123408013101924538041440820171173963 \end{aligned}$$

- The probability that Eve could pass the test is $1/2^4$ since she has a 50-50 chance of guessing correctly for each challenge.

---

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.

- The point is that $m = m^{18-17} = (m^3)^6 \cdot (m^{17})^{-1} \equiv c_B^6 \cdot c_R^{-1} \pmod N$.
- Eve can easily compute both c_B^6 and c_R^{-1} modulo N (the former via successive squaring and the latter via the Euclidean algorithm), so she can quickly obtain m without having to find a factorization of 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?

   - Observe that $(2^e c)^d = 2^{ed} c^d \equiv 2m \pmod{N}$: in other words, the decryption of $2^e c$ is $2m$.
   - So Eve can compute m simply by evaluating $2^{-1} \pmod{N}$ via the Euclidean algorithm and then multiplying w by it.

---

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.]

   - First, we have $1013-1 = 1012 = 2^2 \cdot 11 \cdot 23$. Now we compute $7^{1012} \equiv 1 \pmod{1013}$, but $7^{1012/2} \equiv -1 \pmod{1013}$, $7^{1012/11} \equiv 840 \pmod{1013}$, and $7^{1012/23} \equiv 990 \pmod{1013}$. So by part (b), this means 1013 is prime.
   - For 2027, we have $2026 = 2 \cdot 1013$ and 1013 is prime by the above. Now we compute $7^{2026} \equiv 1 \pmod{2027}$ but $7^{2026/2} \equiv -1 \pmod{2027}$ and $7^2 \equiv 49 \pmod{2027}$. So by part (b), this means 2027 is prime.

   (b) 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.)

   - To apply the criterion we first need to factor $N-1$.
   - Using FactorInteger produces the factorization $N-1 = 2^{15}3^{13}7^{12}11^{13}13 \cdot 1013^7 2027^{11}$, and 1013 and 2027 are prime by (a).
   - Then we must compute the following values modulo N:

$$\begin{aligned}
a^{N-1} &\equiv 1 \\
a^{(N-1)/2} &\equiv -1 \\
a^{(N-1)/3} &\equiv 709729274263082829289661469978323780615812896318322643728828803685814166253235090218971573 28 \\
a^{(N-1)/7} &\equiv 511988274222857596429898210663052019771207667414886091839314224693774536755678906794441864857 \\
a^{(N-1)/11} &\equiv 736908042641603289170515640322561601868923881259488267995239604664349446884174116046604565017 \\
a^{(N-1)/13} &\equiv 459504551413244721489438239305022768327589729306817216271694350492982930307794167935207965709 \\
a^{(N-1)/1013} &\equiv 736157845610144004762183977115470779366440984764453242434674106757868687336658309503192600 70 \\
a^{(N-1)/2027} &\equiv 901572120899637776275344460956505179240965069310204835660786847304328732640222061606010326 28
\end{aligned}$$

   - Since $a^{N-1} \equiv 1$ but $a^{(N-1)/q} \not\equiv 1$ for any prime divisor q of $N-1$, the Lucas criterion therefore says that N is prime.

---

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.]

   - Suppose $k \equiv d \pmod{p-1}$ and $k \equiv d \pmod{q-1}$: we first show $m^{ek} \equiv m \pmod{p}$.
   - If $m \equiv 0 \pmod{p}$ we are done. Otherwise, we have $m^{p-1} \equiv 1 \pmod{p}$.
   - Then since $k \equiv d \pmod{p-1}$ we see that $k = d + (p-1)u$ for some integer u, so we have

     $$m^{ek} = m^{e(d+(p-1)u)} = m^{ed} \cdot (m^{p-1})^u \equiv m \cdot 1^u \equiv m \pmod{p}$$

     since by construction $m^{ed} \equiv m \pmod{p}$.
   - So in either case, $m^{ek} \equiv m \pmod{p}$. By the same argument, $m^{ek} \equiv m \pmod{q}$. Combining the two statements with the Chinese Remainder Theorem gives $m^{ek} \equiv m \pmod{N}$, so k is a decryption exponent.

   (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.]

   - Suppose m is a primitive root mod p. By assumption, $m^{ek} \equiv m \pmod{p}$ so $m^{ek-1} \equiv 1 \pmod{p}$.
   - By properties of order, since m has order $p-1$ mod p then $m^{ek-1} \equiv 1$ if and only if $p-1$ divides $ek-1$, which is to say, when $ek \equiv 1 \pmod{p-1}$.
   - But now since $d \equiv e^{-1} \pmod{\varphi(N)}$ so in particular $e^{-1} \equiv d \pmod{p-1}$: then multiplying $ek \equiv 1 \pmod{p-1}$ by e^{-1} yields $k \equiv d \pmod{p-1}$.
   - By the same argument (taking m to be a primitive root mod q) we see $k \equiv d \pmod{q-1}$ also.

   (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.

   - By (a) and (b), we want to find the solutions to the congruences $x \equiv d \pmod{p-1}$, $x \equiv d \pmod{q-1}$, which are $x \equiv 30491 \pmod{45736}$ and $x \equiv 36251 \pmod{54376}$.
   - By Mathematica's ChineseRemainder command, the solution is $x \equiv \boxed{103622531} \pmod{310867592}$. (The full list of exponents is $103622531 + 310867592u$: Bob's corresponds to $u = 5$.)

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 $\varphi(N)$.
