Suggested reading: Trappe-Washington 3.5–3.6, 1.1–1.2, 6.1

1. (a) Describe the method in Section 3.5 for efficiently computing exponentials $a^b \pmod n$, and verify the book's claim that this can be done in at most $2\log_2(b)$ multiplications.

   (b) Use this method to compute $3^{172} \pmod{191}$.

2. (a) State Fermat's Little Theorem. Define Euler's totient function ϕ, and state Euler's Theorem.

   (b) Use the theorems to describe how we can further simplify the computation of $a^b \pmod n$ when b is larger than $\phi(n)$.

   (c) Noting that 101 is prime, compute

   $$3^{37,123,878,237,982,731,602} \pmod{101}$$

   Show your work. *Hint:* Your solution should be very short.

   (d) Describe how Fermat's Little Theorem can be used as a *primality test*. Explain why it can sometimes be used to verify that an integer n is composite, but it cannot guarantee that a prime integer is prime.

3. Let $n > 0$ be an integer. Recall that we proved that if $[a]$ is a unit modulo n, then "multiplication by $[a]$" is a one-to-one function on the set $\mathbb{Z}/n\mathbb{Z}$.

   (a) Prove that if $[a]$ and $[b]$ are units modulo n, then their product is also a unit. Conclude that "multiplication by $[a]$" is bijective map from the set of units in $\mathbb{Z}/n\mathbb{Z}$ to the set of units in $\mathbb{Z}/n\mathbb{Z}$. *Hint:* Given that $[a]$ has an inverse $[a]^{-1}$ and $[b]$ has an inverse $[b]^{-1}$ modulo n, can you write down an inverse for the product $[a][b]$?

   (b) Prove Euler's Theorem.
   Hint: You can prove it in a way very similar to our proof in lecture of Fermat's Little Theorem. You can also take a look at the proof on pages 82-83 on the textbook, but be sure to write your solution in your own words.

4. A function $\psi : \mathbb{Z} \to \mathbb{Z}$ is called *multiplicative* if $\psi(mn) = \psi(m)\psi(n)$ whenever $\gcd(m, n) = 1$. In this question we will show that Euler's totient function ϕ is multiplicative, and use this fact to derive Euler's product formula for $\phi(N)$.

   (a) Let $p, b \in \mathbb{Z}$, let p be prime and $d > 0$. Use the definition of ϕ to compute $\phi(p)$, and compute $\phi(p^d)$.

   (b) Let $m, n \in \mathbb{Z}$ such that $\gcd(m, n) = 1$. One way to phrase the Chinese Remainder Theorem is to say that the map

   $$\begin{aligned}(\mathbb{Z}/mn\mathbb{Z}) &\longrightarrow (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \\ c \pmod{nm} &\longmapsto \Big(c \pmod m \,,\; c \pmod n \Big)\end{aligned}$$

   is a bijection between the set $(\mathbb{Z}/mn\mathbb{Z})$ and the product of sets $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$.

   Show that this map also defines a bijection between the units in $(\mathbb{Z}/mn\mathbb{Z})$ and the set of pairs of units in $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$. In other words, show that c is invertible modulo nm if and only if it is invertible both modulo n and modulo m.

   (c) Use the result of part (b) to show that ϕ is multiplicative: if $\gcd(m, n) = 1$, then $\phi(mn) = \phi(n)\phi(m)$.

   (d) Combine the results of parts (a) and (c) to show that if N factors as a product of primes

   $$N = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$$

   $$\text{then} \qquad \phi(N) = \Big(p_1^{d_1-1}(p_1-1)\Big)\Big(p_2^{d_2-1}(p_2-1)\Big)\cdots\Big(p_k^{d_k-1}(p_k-1)\Big)$$

(e) Conclude that

$$\phi(N) = N\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

5. (a) Define *public key cryptography*, and describe the RSA cryptosystem. Explain why the decryption method will successfully recover the message in the case that $\gcd(m, n) = 1$.

   (b) Explain the basis for the security of the cipher: which computations are relative efficient, and which are computationally intractable?

6. You publish an RSA encryption modulus $n = 1,367,651$ and exponent $e = 584,377$. Your colleague sends you an encrypted message $1,235,813$. Given that you know the factorization of $n = (701)(1951)$, find a decryption exponent d, and decrypt the message. Show your work.

7. Read about the *Fermat factorization method*. This is the first two paragraphs of Section 6.4, starting on page 181.

   (a) Explain the Fermat factorization method.

   (b) Verify that when n is the product of primes pq, this method will take $\frac{1}{2}|p - q|$ steps to factor n.

   (c) Explain (in a sentence) the implications for selection criteria for the primes p and q in RSA.

8. Our discussion of RSA in class did not address what happens in the (extremely unlikely) case the plaintext m and the encryption modulus n are not coprime. Fortunately, in this case, Bob is still able to recover the message. The following comes from Question 19 in Chapter 6 of the textbook. Assume $n = pq$ is the product of large, distinct primes.

   (a) Suppose that r is a multiple of $\phi(n)$. Show that if m is a unit modulo n, then $m^r \equiv 1 \pmod{p}$ and $m^r \equiv 1 \pmod{q}$.

   (b) Now, with r as above, prove that **any** class m modulo n satisfies $m^{r+1} \equiv m \pmod{p}$ and $m^{r+1} \equiv m \pmod{q}$. *Hint:* You can proceed in cases. If m is not a unit, what must m be modulo a prime?

   (c) Let e and d be encryption and decryption exponents for n. Show that $m^{ed} \equiv m \pmod{n}$ for **any** plaintext m. *Hint:* Recall that p and q are distinct. Apply the Chinese Remainder Theorem.

9. **(Bonus)** The following code is encrypted with an affine cipher. Since the message's creator made the poor choice to leave spaces, you have a good chance of identifying the word "a", and from there, the words "and" and "the".

   St ntjv vmsvos skv gvbxsr ta oxjgvi skvtir nvvjn st gv ivebsvq st skv ltosibq-plspto gvshvvo skv npjyeplpsr ta skv posvfvin boq skv ltjyeplbsvq nsixlsxiv ta skv yipjvn, skvpi gxpeqpof getlzn. Skpn kbn behbrn bssiblsvq yvtyev.
   - B Zobxa

   Ot gibolk ta oxjgvi skvtir pn jtiv nbsxibsvq hpsk jrnsvir skbo skv nsxqr ta yipjv oxjgvin: sktnv vmbnyvibspof, xoixer posvfvin skbs ivaxnv st gv qpcpqvq vcvoer gr bor posvfvin vmlvys skvjnvecvn boq tov. Ntjv yitgevjn ltolviopof yipjvn biv nt npjyev skbs b lkpeq lbo xoqvinsboq skvj boq rvs nt qvvy boq abi aitj ntecvq skbs jbor jbskvjbsplpbon oth nxnyvls skvr kbcv ot ntexspto.
   - J Fbiqovi

   Skviv biv sht ablsn bgtxs skv qpnsipgxspto ta yipjv oxjgvin hkplk P ktyv st ltocpolv rtx nt tcvihkvejpofer skbs skvr hpee gv yvijbovoser vofibcvq po rtxi kvbisn. Skv apins pn skbs qvnypsv skvpi npjyev qvapopspto boq itev bn skv gxpeqpof getlzn ta skv obsxibe oxjgvin, skv yipjv oxjgvin... fith epzv hvvqn bjtof skv obsxibe oxjgvin, nvvjpof st tgvr ot tskvi ebh skbo skbs ta lkbolv, boq otgtqr lbo yivqpls hkviv skv ovms tov hpee nyitxs. Skv nvltoq ablsn pn

VCVO JTIV BNSTOPNKPOF, ATI PS NSBSVN UXNS SKV TYYTNPSV: SKBS SKV YIPJV OXJGVIN VMKPGPS NSXOOPOF IVFXEBIPSR, SKBS SKVIV BIV EBHN FTCVIOPOF SKVPI GVKBCPTXI, BOQ SKBS SKVR TGVR SKVNV EBHN HPSK BEJTNS JPEPSBIR YIVLPNPTO.
- Q WBFPVI

Decipher the message. Outline the steps you use to do so. You do not need to write out the whole message, but show you were succesful by writing the names of the three people quoted.

10. **(Bonus).** A *binary operation* on a set S is a function that takes two elements of S and returns a single element of S. For example, addition $+$ and multiplication $\times$ are both binary operations on the integers.

    A set G with a binary operation $\bullet$ is called a *group* if it satisfies the following axioms:

    i. **Associativity.** For all a, b and c in G, $(a \bullet b) \bullet c = a \bullet (b \bullet c)$.

    ii. **Identity.** There exists an element e in G, called the *identity element*, such that $e \bullet a = a \bullet e = a$ for any element a in G.

    iii. **Inverses.** For each a in G, there exists an inverse element b in G such that $a \bullet b = b \bullet a = e$, where e is the identity element.

    Some examples of groups: the integers (under addition), the nonzero rational numbers (under multiplication), invertible 2×2 matrices (under matrix multiplication), permutations of a finite set (under composition of functions).

    (a) Prove that the set $\mathbb{Z}/n\mathbb{Z}$ is a group under addition. You can assume without proof that addition is associative. You must show:

    * $\mathbb{Z}/n\mathbb{Z}$ has an additive identity.
    * Every element of $\mathbb{Z}/n\mathbb{Z}$ has an additive inverse.

    (b) Prove that for any integer n, the set $\mathbb{Z}/n\mathbb{Z}$ is *not* a group under multiplication. Show explicitly how at least one axiom fails.

    (c) Prove that, for any integer $n > 1$, the set of units in $\mathbb{Z}/n\mathbb{Z}$ form a group under multiplication. You can assume without proof that multiplication is associative. This means you must prove:

    * The product of any two units is a unit. *Hint:* Write down an inverse for the product.
    * $\mathbb{Z}/n\mathbb{Z}$ has a multiplicative identity which is a unit.
    * Every unit has a multiplicative inverse, which is also a unit.

    This group is called the *group of units* of $\mathbb{Z}/n\mathbb{Z}$, and is sometimes denoted $(\mathbb{Z}/n\mathbb{Z})^\times$.

    (d) Let G be a group with operation $\bullet$. Lagrange's theorem states that if G has $|G|$ elements (a finite number), and $g \in G$ is any element, then $g \bullet g \bullet \cdots \bullet g$ (with $|G|$ factors) is the identity element. Assuming Lagrange's theorem, reprove Euler's theorem: $a^{\phi(n)} \equiv 1 \pmod{n}$ for any unit $a \pmod{n}$.