Math 110 Homework 3 Solutions

January 29, 2015

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 $3^{172} \pmod{191}$.

   Solution: (a) The basic idea is that a^{2^m} can be calculated in $m-1$ multiplications, as $a^{2^m} \equiv a^{2^{m-1}} \cdot a^{2^{m-1}} \pmod n$ so you can multiply the exponent by two by doing one multiplication. In general, write $b = c_m \cdot 2^m + c_{m-1} \cdot 2^{m-1} + \ldots + c_1 2 + c_0$ where $c_i \in \{0, 1\}$. Then compute $a, a^2, a^4, \ldots, a^{2^m} \pmod n$ by multiplying the previous element in this list with itself. This takes $m-1$ multiplications. Finally compute

   $$a^{c_m 2^m} \cdot a^{c_{m-1} 2^{m-1}} \cdot \ldots \cdot a^{2c_1} \cdot a^{c_0} \equiv a^b \pmod n$$

   This requires at most m multiplications, as each term is either 1 or one of the precomputed a^{2^i}. Note that m is the integer part of $\log_2(b)$, so we need at most $2\log_2(b)$ multiplications.

   (b) For example, $172 = 128 + 32 + 8 + 4$, and

   $$\begin{aligned} 3^4 &\equiv 81 \pmod{191} \\ 3^8 &\equiv 67 \pmod{191} \\ 3^{16} &\equiv 96 \pmod{191} \\ 3^{32} &\equiv 48 \pmod{191} \\ 3^{64} &\equiv 12 \pmod{191} \\ 3^{128} &\equiv 144 \pmod{191} \end{aligned}$$

   Therefore we combine these to see that

   $$3^{172} \equiv 144 \cdot 48 \cdot 67 \cdot 81 \equiv 170 \pmod{191}.$$

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.

Solution: (a) Here are the theorem statements and definition as they appear when typesetting using theorem environment in LaTeX.

Theorem 1 (Fermat's Little Theorem)**.** *Let p be a prime and a be an integer which is not a multiple of p. Then $a^{p-1} \equiv 1 \pmod{p}$.*

Definition 2. Let n be a positive integer. The Euler totient of n, denoted $\phi(n)$, is the number of positive integers less than n which are relatively prime to n. Equivalently, $\phi(n)$ is the number of units in $\mathbb{Z}/n\mathbb{Z}$.

Theorem 3 (Euler's Theorem)**.** *Let n be a positive integer and a an integer relatively prime to n. Then $a^{\phi(n)} \equiv 1 \pmod{n}$.*

(b) This allows simplifications of the computation of $a^b \pmod{n}$, because if $b \equiv b' \pmod{\phi(n)}$, $a^b \equiv a^{b'} \pmod{n}$. To see this, just write $b = b' + t\phi(n)$ for an integer t, and compute

$$a^b \equiv a^{b'+t\phi(n)} \equiv a^{b'} \left(a^{\phi(n)}\right)^t \equiv a^{b'} \pmod{n}.$$

This means we can replace a general b with its least residue modulo $\phi(n)$, an integer between 0 and $\phi(n)$, which will potentially be much smaller than b.

(c) In the case that $n = 101$, the exponent matters only modulo 100. Since the exponent is congruent to 2 (mod 100), the answer is $3^2 \equiv 9 \pmod{101}$.

(d) Taking the contrapositive of Fermat's little theorem, if there an a and p such that $a^{p-1} \not\equiv 1 \pmod{p}$, it would follow that p is not prime. So to test whether a number is not prime, one can simply search for an a where this happens; $a = 2$ is a good starting place. If you find one, it is not prime. If you can't find any, then it is highly likely that p is prime, but not guaranteed. In fact, there are integers that are not prime and where no such a exists: they are called Carmichael numbers.

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.

Solution: (a) Since $[a]$ and $[b]$ have inverses, consider the congruence class $[a]^{-1}[b]^{-1}$. Then

$$[a][b]([a]^{-1}[b]^{-1}) = [a][a]^{-1}[b][b]^{-1} = [1],$$

and the same computation shows that $([a]^{-1}[b]^{-1})[a][b] = 1$. Hence $[a][b]$ is a unit.

Let f be the multiplication by $[a]$ map: it sends $[b] \to [a][b]$. By Part(a), if $[b]$ is a unit then $[a][b]$ is as well. It is injective because if $f([b]) = f([b'])$ then $[a][b] = [a][b']$. Multiplying by $[a]^{-1}$, we see $[b] = [b']$. It is surjective because given a unit $[b]$, $f([a]^{-1}[b]) = [b]$. We conclude that f gives a bijective map from the set of units in $\mathbb{Z}/n\mathbb{Z}$ to itself.

(b) Now let n be a positive integer and let a be relatively prime to n. This means $[a]$ is a unit. Let $(\mathbb{Z}/n\mathbb{Z})^\times$ denote the set of units modulo n . Remember that it contains $\phi(n)$ elements as having an inverse modulo n means an integer is relatively prime to n. Consider the product

$$P = \prod_{b \in (\mathbb{Z}/n\mathbb{Z})^\times} [b]$$

Because f is a bijection, the elements $[a][b] = f([b])$ for $b \in (\mathbb{Z}/n\mathbb{Z})^\times$ are exactly the units modulo n, just in a different order. Therefore

$$\prod_{b \in (\mathbb{Z}/n\mathbb{Z})^\times} [b] = P = \prod_{b \in (\mathbb{Z}/n\mathbb{Z})^\times} [a][b] = [a]^{\phi(n)} \prod_{b \in (\mathbb{Z}/n\mathbb{Z})^\times} [b]$$

Canceling out the P, we see $a^{\phi(n)} \equiv 1 \pmod{n}$.

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

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

Solution: (a) First let p be prime. Every positive integer less than p is relatively prime to p, so $\phi(p) = p - 1$. Likewise, the only positive integers less than p^d that share a factor with p^d are the multiples of p:

$$p, \; 2p, \; 3p, \; \ldots (p^{d-1})p$$

We count p^{d-1} of these multiples. Therefore

$$\phi(p^d) = p^d - p^{d-1} = p^{d-1}(p - 1).$$

(b) Recall that a is a unit modulo n if and only if $\gcd(a, n) = 1$. So if a is a unit modulo mn, it does not share any divisors with m and n and hence is a unit modulo m and n. Conversely, suppose a is not invertible modulo mn. This means there is a common divisor, which we may take to be prime. Thus

$p|a$ and $p|mn$. But this means $p|m$ or $p|n$ as p is prime, hence a shares a common divisor with m or n. This means a is not invertible modulo m or n.

An alternative way to prove this fact: Assume that $\gcd(a, nm) = 1$. This means that there exist integers u, v so that $au + mnv = 1$. Any common divisor d of a and m divides both terms on the left-hand side of this equation, and so d divides 1. Similarly any common divisor of a and n divides 1, and we conclude that $\gcd(a, m) = 1 = \gcd(a, n) = 1$. Conversely, if $\gcd(a, m) = 1$ and $\gcd(a, n) = 1$ then there are integers u, v, x, y so that

$$au + mv = 1 \qquad \text{and} \qquad ax + ny = 1.$$

Multiplying these equations together, we find

$$1 = (ax + ny)(au + mv) = axau + axmv + nyau + nymv = a(xau + xmv + nyu) + (mn)(yv)$$

and we conclude that $\gcd(a, mn) = 1$.

By the Chinese Remainder Theorem, we already knew 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 one-to-one and onto. Now we know that it maps every unit $c \pmod{mn}$ to a pair of units $\Big(c \pmod{m} \ , \ c \pmod{n} \Big)$, and conversely that every pair of units is in the image of a unit $c \pmod{mn}$. We conclude that the map restricts to a bijection between the set of units in $(\mathbb{Z}/mn\mathbb{Z})$ and the set of pairs of units in $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$.

(c) Denote the units modulo n by $(\mathbb{Z}/n\mathbb{Z})^\times$. Since there is a bijection

$$(\mathbb{Z}/nm\mathbb{Z})^\times \simeq (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times,$$

the two sets have the same number of elements. As an integer is a unit if and only if it relatively prime to the modulus, $(\mathbb{Z}/nm\mathbb{Z})^\times$ has $\phi(mn)$ elements while $(\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$ has $\phi(m)\phi(n)$ elements. Note this relied on the isomorphism given by the Chinese remainder theorem, which requires m and n to be relatively prime.

(d) Now we combine the previous parts. Write $N = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$. Then using that ϕ is multiplicative, we see

$$\phi(N) = \phi(p_1^{d_1})\phi(p_2^{d_2} \dots p_k^{d_k}) = \dots = \phi(p_1^{d_1})\phi(p_2^{d_2}) \dots \phi(p_k^{d_k}).$$

Now using the first part about prime powers on each of the terms, we see

$$\phi(N) = p_1^{d_1 - 1}(p_1 - 1) \dots p_k^{d_k - 1}(p_k - 1).$$

(e) Finally pulling out a $p_i^{d_i}$ from each term, we see

$$\begin{aligned} \phi(N) &= p_1^{d_1} p_2^{d_2} \dots p_k^{d_k} p_1^{-1}(p_1 - 1) p_2^{-1}(p_2 - 1) \dots p_k^{-1}(p_k - 1) \\ &= N(1 - p_1^{-1})(1 - p_2^{-1}) \dots (1 - p_k^{-1}). \end{aligned}$$

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?

Solution: (a) This is discussed in full detail at the beginning of Chapter 6 of the textbook. The key points are that public key cryptography is a way for Alice and Bob to communicate without having to share any common secret and without an eavesdropper Eve being able to learn anything about what they are saying. RSA is the most famous example of this. Bob picks two large primes p and q, and computes $n = pq$. Furthermore, Bob picks an integer e which is invertible modulo $\phi(n) = (p-1)(q-1)$, and computes a multiplicative inverse d modulo $\phi(n)$. Bob tells everyone n and e, but keeps p, q, and d secret.

Alice can send a number $M \pmod{n}$ to Bob by computing $M^e \pmod{n}$. Bob can decrypt it by raising to the dth power, as $M^{ed} \equiv M \pmod{n}$ (this uses Euler's theorem and $ed \equiv 1 \pmod{(p-1)(q-1)}$).

(b) By Problem 1, all of the powers are computationally efficient to compute, and it is easy to find an multiplicative inverse to e modulo $(p-1)(q-1)$ using the Euclidean algorithm. It is also computationally efficient to check whether a number is prime, and a random number is likely enough to be prime that Bob can simply try random number until one is prime to efficiently find p and q to use: we are not in a position to justify these assertions now. So there are no computational problems to using RSA.

In order to break RSA, the only obvious line of attack would be to compute d. We need to invert e modulo $\phi(n)$ to do so. There is no obvious way to compute $\phi(n)$ without knowing the factorization of n, which was kept secret. It is thought to be computationally intractable to factor n if p and q are randomly chosen large primes, so RSA looks hard. However, no one has methods to prove that breaking RSA is actually 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.

   Solution: The first step is to find a multiplicative inverse of e modulo $\phi(n) = 700 \cdot 1950$. Using the Euclidean algorithm gives $d = 313 \pmod{n}$. To decrypt the message, just compute $(1235813)^d \equiv 220813 \pmod{n}$ as in problem 1.

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.

   Solution: (a) Refer to the discussion in the textbook.

   (b) Given n, the method checks whether $n + x^2$ is a perfect square for $x = 1, 2, \ldots$. If it were, $n = y^2 - x^2 = (y+x)(y-x)$. After possibly swapping p and q, we may suppose $p < q$. Then given this factorization, $y - x = p$ and $y + x = q$ using unique prime factorization. Solving this system for x, we see $x = \frac{q-p}{2}$. This is how long we search for $n + x^2$ to be a perfect square.

   (c) The existence of this factorization method means that if the p and q chosen for RSA satisfy $|p-q| = s$, it is feasible to factor n in time polynomial in s. So we must pick p and q sufficiently far apart, say $p > 2q$, to avoid this being feasible.

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.

Solution: (a) We can write $r = k\phi(n) = k(p-1)(q-1)$ for some $k \in \mathbb{Z}$. Then by Fermat's Little Theorem,

$$m^r = m^{k(p-1)(q-1)} = (m^{p-1})^{k(q-1)} \equiv 1^{k(q-1)} \pmod{p} \equiv 1 \pmod{p}.$$

Similarly, $m^r = (m^{q-1})^{k(p-1)} \equiv 1 \pmod{q}$.

(b) First suppose that m is not a unit modulo p. This implies that m is congruent to zero, so it is immediate that

$$m^{r+1} \equiv 0^{r+1} \pmod{p} \equiv 0 \pmod{p} \equiv m \pmod{p}.$$

Similarly if m is not a unit modulo q then m is congruent to zero and $m^{r+1} \equiv m \pmod{q}$.

Alternatively, if m is a unit modulo p, then by Part (a) $m^r \equiv 1 \pmod{p}$, so multiplying through by m we find $m^{r+1} \equiv m \pmod{p}$. The same argument shows that if m is a unit modulo q then $m^{r+1} \equiv m \pmod{q}$.

(c) Let e and d be encryption exponents for the RSA modulus n, that is, $ed \equiv 1 \pmod{\phi(n)}$. This means that the integer ed is of the form $r+1$ for some multiple r of $\phi(n)$. By Part (b), it follows that

$$m^{ed} = m^{r+1} \equiv m \pmod{p} \qquad \text{and } m^{ed} = m^{r+1} \equiv m \pmod{q}.$$

By the Chinese Remainder Theorem, $[m]$ is the only congruence class modulo $n = pq$ that simultaneously reduces to $m \pmod{p}$ and $m \pmod{q}$, and so Bob must successfully recover the message $m^{ed} \equiv m \pmod{n}$.

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 abls 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.

Solution: We identify from the second quotation that 'B' likely encodes 'a', and so the frequently appearing three-letter words 'BOQ' and 'SKV' are likely 'and' and 'the', respectively.

Using the same method from Homework 2, we determine that the affine encryption function is $f(x) = 5x + 1$. The decrypted message is:

> To some extent the beauty of number theory seems to be related to the contradiction between the simplicity of the integers and the complicated structure of the primes, their building blocks. This has always attracted people.
> - A Knauf

> No branch of number theory is more saturated with mystery than the study of prime numbers: those exasperating, unruly integers that refuse to be divided evenly by any integers except themselves and one. Some problems concerning primes are so simple that a child can understand them and yet so deep and far from solved that many mathematicians now suspect they have no solution.
> - M Gardner

> There are two facts about the distribution of prime numbers which I hope to convince you so overwhelmingly that they will be permanently engraved in your hearts. The first is that despite their simple definition and role as the building blocks of the natural numbers, the prime numbers... grow like weeds among the natural numbers, seeming to obey no other law than that of chance, and nobody can predict where the next one will sprout. The second fact is even more astonishing, for it states just the opposite: that the prime numbers exhibit stunning regularity, that there are laws governing their behaviour, and that they obey these laws with almost military precision.
> - D Zagier

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 $a \pmod{n}$.

Solution: (a) Let $[a] \in \mathbb{Z}/n\mathbb{Z}$. The additive inverse for $[a]$ is $[-a]$, and the identity element is $[0]$.

(b) Note that $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication because $[0]$ (or any element which shares a factor with n) does not have a multiplicative inverse.

(c) For the units modulo n, Question 3 showed why the product of units is a unit. $[1]$ is the multiplicative identity. The inverse for the group operation is just the multiplicative inverse.

(d) Recall that $|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n)$ because the numbers less than n which are relatively prime to n are exactly those which are units. Let a be an integer which is relatively prime to n. It is a unit, so $[a] \in (\mathbb{Z}/n\mathbb{Z})^\times$ satisfies $[a]^{\phi(n)} = [1]$ by Lagrange's theorem.