Mathematics 243, section 3 – Algebraic Structures
Solutions for Problem Set 7

'A' Section

1. If we are using an affine cypher and we want to include *more symbols* in our plaintext messages than just the capital letters and a blank space as in the examples we did in class, then we can do that by increasing the modulus m for the numerical form of our plain and cypher text. For this problem, say we want to include the letters $A, B, C, \ldots, Z$, the space , and the apostrophe, comma, period, and question mark. Then we can use $\mathbb{Z}_{31}$ as the numerical form of our alphabet, and make $A \leftrightarrow 0$, $B \leftrightarrow 1, \ldots, Z \leftrightarrow 25$, the space be 26, the apostrophe be 27, the comma be 28, the period be 29, and the question mark be 30.

   a. Use the affine encryption function $f(x) = 7x + 20 \pmod{31}$ to encrypt the plaintext message "Are we on for today?" Give the cyphertext in literal form (using the same alphabet).

   Solution: In numerical form, the plain text is:

   $$0, 17, 4, 26, 22, 4, 26, 14, 13, 26, 5, 14, 17, 26, 19, 15, 3, 0, 24, 30$$

   Applying f to each in turn we get

   $$20, 15, 17, 16, 19, 17, 16, 25, 18, 16, 24, 25, 15, 16, 29, 1, 10, 20, 2, 13$$

   For instance, the second symbol of the plain text is $R \leftrightarrow 17$. This maps to

   $$f(17) = 7 \cdot 17 + 20 = 139 \equiv 15 \pmod{31}$$

   since $139 = 4 \cdot 31 + 15$ by division.

   b. What is the decryption function $g = f^{-1}$ for this f?

   Solution: We want $g(x) = Ax + B \pmod{31}$ such that $g(f(x)) \equiv x \pmod{31}$ for all $[x] \in \mathbb{Z}_{31}$. This will be true if $7A \equiv 1 \pmod{31}$ and $B \equiv -20A \pmod{31}$. We find A via the extended Euclidean Algorithm:

   $$\begin{aligned} 31 &= 4 \cdot 7 + 3 \\ 6 &= 2 \cdot 3 + 1. \end{aligned}$$

   Then we fill in the extended Euclidean Algorithm table as follows

   $$\begin{array}{rrr} & 1 & 0 \\ & 0 & 1 \\ 4 & 1 & -4 \\ 2 & -2 & 9 \end{array}$$

   which shows that $[A] = [7]^{-1} = [9]$ in $\mathbb{Z}_{31}$. Then $B \equiv -180 \equiv 6 \pmod{31}$. So $g(x) = 9x + 6 \pmod{31}$. Then $A \equiv \pmod{31}$

c. Use the decryption function to decrypt the cyphertext "SZQOQDUSW." (Note: the period at the end *is part of the cypher text.*)

Solution: The cyphertext converts to numerical form as:

$$18, 25, 16, 14, 16, 3, 20, 18, 23, 29$$

Applying the decryption function $g(x) = 9x + 6 \pmod{31}$ to each number in turn, we get

$$13, 14, 26, 8, 26, 2, 0, 13, 27, 19$$

which corresponds to the plain text "NO I CAN'T"

2. Suppose an RSA public key cryptosystem has $m = 7 \cdot 11 = 77$, and an encryption exponent $e = 7$ is used. Use the 27-letter alphabet (space = 0). from our examples in class and two-digit blocks.

a. Encrypt the plaintext message "GO FOR IT" using this system (Note: the cyphertext will be in numerical, not literal form.)

Solution: The RSA encryption function is $f(x) = x^e = x^7 \pmod{77}$ The plain text (as blocks of length 2) is

$$7, 15, 00, 06, 15, 18, 00, 09, 20$$

which encrypts to

$$28, 71, 00, 41, 71, 39, 00, 37, 48$$

b. What is the ("secret") decryption exponent d for this system?

Solution This is the exponent d that satisfies $7d \equiv 1 \pmod{60}$, where $60 = (7-1)(11-1) = (p-1)(q-1)$. Since $\gcd(7, 60) = 1$, there exists such a d that we can find by applying the extended Euclidean Algorithm:

$$\begin{aligned} 60 &= 8 \cdot 7 + 4 \\ 7 &= 1 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \end{aligned}$$

Then we fill in the extended Euclidean Algorithm table as follows

$$\begin{array}{rrr} & 1 & 0 \\ & 0 & 1 \\ 8 & 1 & -8 \\ 1 & -1 & 9 \\ 1 & 2 & -17 \end{array}$$

The equation is $(2)(60) + (-17)(7) = 1$ and the multiplicative inverse of 7 is $d \equiv -17 \equiv 43 \pmod{60}$. So $g(x) = x^{43} \pmod{77}$.

c. Use it to decrypt the cyphertext: "42, 71, 23, 1, 53, 10, 71, 68, 47" (Why didn't I actually include spaces between the words here?)

Solution: The cyphertext decrypts to

$$14, 15, 23, 1, 25, 10, 15, 19, 5$$

which corresponds to "NOWAYJOSE." Note that 0 is mapped to itself under both the RSA encryption and decryption functions. So the presence of a bunch of zeroes might be extra information that might lead to breaking the code(!)

'B' Section

The Euler ϕ-function (or totient) is defined for $n > 0$ in $\mathbb{Z}$ by $\phi(n)$ = the number of classes $[a]$ in $\mathbb{Z}_n$ for which a multiplicative inverse exists in $\mathbb{Z}_n$ (this is the same as the number of a with $0 \leq a < n$ and $\gcd(a, n) = 1$).

1. Find $\phi(11)$, $\phi(16)$, and $\phi(20)$.

   Solution: $\phi(11) = 10$ since $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ are all relatively prime to 11. $\phi(16) = 8$ since $\{1, 3, 5, 7, 9, 11, 13, 15\}$ are the only integers a with $0 \leq a < 16$ that are relatively prime to 16. Similarly, $\phi(20) = 8$, since $\{1, 3, 7, 9, 11, 13, 17, 19\}$ the a with $0 \leq a < 20$ and $\gcd(a, 20) = 1$.

2. Prove that the number of ordered pairs (a, b) for which $f(x) = ax + b \pmod{n}$ defines an invertible affine encryption function on $\mathbb{Z}_n$ is $n \cdot \phi(n)$.

   Solution: By the proposition about affine encryption functions we proved in class on Wednesday 10/31, we have an inverse function for g as long as $\gcd(a, n) = 1$, or equivalently if $[a]^{-1}$ exists in $\mathbb{Z}_n$. There are thus $\phi(n)$ different choices for a. For each of those, there are n choices for b. Hence we have $n\phi(n)$ possible mappings of this form.

   On the other hand, note that if $\gcd(a, n) = d > 1$, then we claim that $f(x) = ax + b \pmod{n}$ has no inverse function, so it cannot be used as an affine encryption function. This is true because if $\gcd(a, n) = d > 1$ with $n = qd$ and $a = sd$ for integers q, s, then $f(0) = b \pmod{n}$ and $f(q) = aq + b = sdq + b = sn + b \equiv b \pmod{n}$, but $q \not\equiv 0 \pmod{n}$ so f is not a 1-1 mapping on $\mathbb{Z}_n$. (That says, of course, that f is not suitable as an encryption function because it would map different plaintext symbols to the same cyphertext. In that case, unique decryption is impossible!) This shows that there are exactly $\phi(n) \cdot n$ invertible affine mappings.

3. Show that the set of affine encryption functions is closed under composition.

   Solution: Let $f(x) = ax + b \pmod{n}$ and $g(x) \equiv cx + d \pmod{n}$ with $\gcd(a, n) = \gcd(c, n) = 1$ (see problem 2 above). Then

   $$(f \circ g)(x) = a(cx + d) + b = acx + (ad + b) \pmod{n}.$$

This is another mapping of the same form so we have part of what we want. The other thing we must check is that $\gcd(ac, n) = 1$ also. We can see this as follows. Since $\gcd(a, n) = 1$, there are integers p, q such that $pa + qn = 1$. Similarly since $\gcd(c, n) = 1$, there are integers r, s such that $rc + sn = 1$. If we multiply corresponding sides of these equations we get

$$1 = 1 \cdot 1 = (pa + qn)(rc + sn) = (pr)(ac) + (pas + qrc + qns)n.$$

Since $pr, (pas + qrc + qns) \in \mathbb{Z}$, This implies that $\gcd(ac, n) = 1$. (The smallest positive element of the the set $\{P(ac) + Qn \mid P, Q \in \mathbb{Z}\}$ must be 1.)

4. If $n = pq$ where p, q are distinct primes, prove that $\phi(n) = (p - 1)(q - 1)$.

   Solution: The a satisfying $0 \leq a < n$ and $\gcd(a, n) > 1$ in the case $n = pq$ are precisely the multiples of p or q. Let

   $$P = \{0, p, 2p, 3p, \ldots, (q - 1)p\}$$

   and

   $$Q = \{0, q, 2q, 3q, \ldots, (p - 1)q\}.$$

   There are $q = |P|$ numbers of the first kind and $p = |Q|$ numbers of the second kind. We want the number of elements in $\{0, 1, \ldots, n - 1\} - (P \cup Q)$. Since 0 is contained in both lists though, this means that the number of a with $\gcd(a, n) = 1$ is precisely

   $$pq - (p + q - 1) = pq - p - q + 1 = (p - 1)(q - 1).$$

   (We could also remove 0 from the start and count like this: There are $p - 1$ nonzero multiples of q and $q - 1$ nonzero multiples of p in this range. So

   $$\phi(pq) = (pq - 1) - (p - 1) - (q - 1) = pq - p - q + 1 = (p - 1)(q - 1),$$

   as before.

5. If $n = p^e$ where p is prime and $e \geq 1$, then show $\phi(n) = p^e - p^{e-1} = p^{e-1}(p - 1)$.

   Solution: The idea is similar to that of question 4. The numbers a in $0 \leq a < p^e$ that are not relatively prime to $n = p^e$ are precisely the multiples of p in this range. The largest k such that $kp < p^e$ is $k = p^{e-1} - 1$. So we must take out the numbers in $\{0, p, 2p, \ldots, p \cdot p, \cdots, (p^{e-1} - 1)p\}$ to count $\phi(p^e)$. There are p^{e-1} elements in this set and we want the complement in $\{0, 1, \ldots, p^e - 1\}$ Hence the number is

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