CSE 015: Discrete Mathematics
Homework #10
Solution

Arvind Kumar
Lab CSE-015-07L

April 19, 2022

Chapter 4.3

1. **Question 31: Show that if a and b are positive integers, then ab = gcd(a, b) x lcm(a, b). [Hint: Use the prime factorizations of a and b and the formulae for gcd(a, b) and lcm(a, b) in terms of these factorizations.]**

   (a) 31: Let's set a = 18 and b = 42. ab = 756, the factors of a is 1,2,3,6,9,18, and the factors of b is 1,2,3,6,7,14,21,42. The gcd of a and b is 6 and the lcm of a and b is 126. The multiplied value of gcd and lcm is 6 x 126 which is 756m and proves that ab = gcd(a, b) x lcm(a, b).

2. **Question 32: Use the Euclidean algorithm to find**

   (a) 32c: gcd(123, 277), 277 / 123 = 2 remainder 31, 123 / 31 = 3 remainder 30, 31 / 30 = 1 remainder 1, 30 / 1 = 30 remainder 0, so the gcd of 123 and 277 is 1 since it is what is divided by to get a remainder of 0. Answer: 1

   (b) 32d: gcd(1529, 14039), 14039 / 1529 = 9 remainder 278, 1529 / 278 = 5 remainder 139, 278 / 139 = 2 remainder 0, so the gcd of 1529 and 14039 is 139 since the divided value gives a remainder of 0. Answer: 139

   Question 42: Use the extended Euclidean algorithm to express gcd(252, 356) as a linear combination of 252 and 356

   (a) 42: gcd(252, 356) with steps is 356 = 1 x 252 + 104, 252 = 2 x 104 + 44, 104 = 2 x 44 + 16, 44 = 2 x 16 + 12, 16 = 1 x 12 + 4, 16 = 1 x 12 + 4, 12 = 3 x 4, the q_i are $q_1 = 1$, $q_2 = 2$, $q_3 = 2$, $q_4 = 2$, $q_5 = 1$, the extended sets initially are $s_0 = 1$, $s_1 = 0$, $t_0 = 0$, $t_1 = 1$. We will have $s_2 = s_0 - q_1s_1 = 1\text{-}1*0 = 1$, $t_2 = t_0 - q_1t_1 = 0\text{-}1*1 = -1$, $s_3 = s_1 - q_2s_2 = 0\text{-}2*1 = -2$, $t_3 = t_1 - q_2t_2 = 1\text{-}2*\text{-}1 = 3$, $s_4 = s_2 - q_3s_3 = 1\text{-}2*\text{-}2 = 5$, $t_4 = t_2 - q_3t_3 = \text{-}1\text{-}2*3 = -7$, $s_5 = s_3 - q_4s_4 = \text{-}2\text{-}2*5 = -12$, $t_5 = t_3 - q_4t_4 = 3\text{-}2*\text{-}7 = 17$, $s_6 = s_4 - q_5s_5 = 5\text{-}1*\text{-}12 = 17$, $t_6 = t_4 - q_5t_5 = \text{-}7\text{-}1*17 = 24$, we get gcd(252, 356) = 17*356 + (-24)*252.

   Question 50: Show that if a, b, and m are integers such that m $\geq$ 2 and a $\equiv$ b (mod m), then gcd(a, m) = gcd(b, m).

   (a) 50: Lets define A and B as: A = gcd(a,m) and B = gcd(b,m), and the gcd divides two integers as A—a, A—m, B—b, B—m , and since a = mc+b, A—a and A—m implies A—b, and since a = mc+b, B—b and B—m implies B—a, it means that A—gcd(b,m) and B—gcd(a,m). And since A = gcd(a,m) and B = gcd(b,m), so we will have A—B and B—A. This will imply that A = B, so gcd(a,m) = gcd(b,m).

Chapter 4.4

1. **Question 6: Find an inverse of a modulo m for each of these pairs of relatively prime integers using the method followed in Example 2.**

   (a) 6a: a = 2, m = 17, the inverse of a modulo m is an integer b when ab $\equiv$ 1 (mod m) with the Euclidean algorithm is 17 = 8*2+1, 2 = 2*1, and the gcd of a and m is 1. This is shown by gcd(a,m) = 1, 17 - 8*2, 1*17-8*2. and the inverse is the coefficient of a, which is -8. And since -8 mod 17 = 9 mod 17, 9 is also the inverse of a modulo m.

   (b) 6b: a = 34, m = 89, the inverse of a modulo m is an integer b when ab $\equiv$ 1 (mod m) with the Euclidean algorithm is 89 = 2*34+21, 34 = 1*21+13, 21 = 1*13+8, 13 = 1*8+5, 8 = 1*5+3, 5 = 1*3+2, 3 = 1*2+1, 2 = 2*1. The greatest common divisor of a and m is 1, and we can write this out as a multiple of a and m. gcd(a,m) = 1, = 3-1*2, 1*3-1*2 = 1*3-1*(5-1*3) = 2*3-1*5 = 2*(8-1*5)-1*5, 2*8-3*5 = 5*8-3*13 = 5*(21-1*13)-3*13 = 5*21-8*13 = 13*21-8*34 = 13*(89-2*34)-8*34 = 13*89-34*34. The inverse is the coefficient of a, which is -34. Since -34 mod 89 = -34 + 89 mod 89 = 55 mod 89, 55 is also the inverse of a modulo m.

   Question 10: Solve the congruence 2x $\equiv$ 7 (mod 17) using the inverse of 2 modulo 17 found in part (a) of Exercise 6.

   (a) 10: We can show this with 9 x 2x $\equiv$ = 9 x 7 (mod 17), 18x $\equiv$ 63 (mod 17) with $\equiv$ 12(mod 17), the solution of the congruence.

   Question 12: Solve each of these congruences using the modular inverses found in parts (b), (c), and (d) of Exercise 6.

   (a) 12a: 34x $\equiv$ 77 (mod 89), a = 34, m = 89. With the Euclidean: 89 = 2*34+21, 34 = 1*21+13, 21 = 1*13+8, 13 = 1*8+5, 8 = 1*5+3, 5 = 1*3+2, 3 = 1*2+1, 2 = 2*1, And we have gcd(a,m) = 1, 1*3-1*2, 1*3-1(5-1*3), 2*3-1*5, 2(8-1*5)-1*5, 2*8-3*5, 2*8-3*(13-1*8), 5*8-3*13, 5*(21-1*13)-3*13, 5*21-8*13, 5*21-8*(34-1*21), 13*21-8*34, 13*(89-2*34)-8*32, 13*89-34*34. The inverse of the coefficient of a is -34. And since -34 mod 89 = -34 + 89 mod 89 = 55 mod 89, then 55 is also the inverse of modulo m. Now we multiply 55 on both sides on the equation and we use 34*55 mod 89 = 1: 55*34*x $\equiv$ 55$\equiv$77(mod 89), x $\equiv$4235(mod 89), x $\equiv$ 52(mod 89).

Chapter 4.5

1. **Question 2: Which memory locations are assigned by the hashing function h(k) = k mod 101 to the records of insurance company customers with these Social Security numbers?**

   (a) 2a: 104578690, h(104578690) = 104578690 mod 101, 104578690 / 101 = 1035432.574, 1035432*101 = 104578632, 104578690 - 104578632 = 58, so h(104578690) = 58.

   (b) 2b: 432222187, h(432222187) = 432222187 mod 101, 432222187 / 101 = 4279427.594, 4279427*101 = 432222127, 432222187 = 432222127 = 60, so h(432222187) = 60.

2. **Question 6: What sequence of pseudorandom numbers is generated using the linear congruential generator $x_{n+1} = (4x_n + 1) \bmod 7$ with seed $x_0 = 3$?**

   (a) 6: x_0 = 3, n = 0, x_1 = (13) mod 7 = 6, n = 1, x_2 = (25) mod 7 = 4, n = 2, x_3 = (17) mod 7 = 3, n = 3, x_4 = (13) mod 7 = 6, n = 4, x_5 = (25) mod 7 = 4, n = 5, x_6 = (17) mod 7 = 3, n = 6, x_7 = (13) mod 7 = 6, and the sequence is 6,4,3,6,4,3,6,...

Chapter 4.6

1. **Question 2: Encrypt the message STOP POLLUTION by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.**

   (a) 2a: f(p) = (p + 4) mod 26, lets set A = 0, B = 1, and so on until Z = 25. STOP POLLUTION would be converted as (18 19 14 15 15 14 11 11 20 19 8 14 13), and adding 4 to each value would give us (22 23 18 19 19 18 15 15 24 23 12 18 17), which converted back to letters would be WXST TSPPYXMSR.

2. **Question 4: Decrypt these messages that were encrypted using the Caesar cipher.**

   (a) 4a: EOXH MHDQV, Lets set A = 0, B = 1, C = 2, until Z = 25, lets do the combinations by shifting every key up by one. We need to do 25 shifts, because there are 26 letters in the alphabet, and EOXH MHDQV would be the same at the 26th shift. The 1st shift: FPYI NIERW, The 2nd shift: GQZJ OJFSX, The 3rd shift: HRAK PKGTY, The 4th shift: ISBL QLHUZ, The 5th shift: JTCM RMIVA, The 6th shift: KUDN SNJWB, The 7th shift: LVEO TOKXC, The 8th shift: MWFP UPLYD, The 9th shift: NXGQ VQMZE, The 10th shift: OYHR WRNAF, The 11th shift: PZIS XSOBG, The 12th shift: QAJT YTPCH, The 13th shift: RBKU ZUQDI, The 14th shift: SCLV AVREJ, The 15th shift: TDMW BWSFK, The 16th shift: UENX CXTGL, The 17th shift: VFOY DYUHM, The 18th shift: WGPZ EZVIN, The 19th shift: XHQA FAWJO, The 20th shift: YIRB GBXKP, The 21th shift: ZJSC HCYLQ, The 22th shift: AKTD IDZMR, The 23th shift: BLUE JEANS, The 24th shift: CMVF KFBOT, The 25th shift: DNWG LGCPU, Out of all the shifts here, BLUE JEANS is the only combination that is a message that one could understand. It took 23 shifts up and 3 shifts down. This means that the Caesar cipher is f(p) = (p+3) mod 26 for BLUE JEANS, and the inverse is $f^{-1}(p)$ = (p-3) mod 26 required to decrypt the encrypted message EOXH MHDQV.