CSCE 222 (Carlisle), Discrete Structures for Computing
Spring 2020
Homework 12

Type your name below the pledge to sign
On my honor, as an Aggie, I have neither given nor received unauthorized aid on this academic work.
Arthur Chen

Instructions:

- The exercises are from the textbook. You are encouraged to work extra problems to aid in your learning; remember, the solutions to the odd-numbered problems are in the back of the book.
- Grading will be based on correctness, clarity, and whether your solution is of the appropriate length.
- Always justify your answers.
- Don't forget to acknowledge all sources of assistance in the section below, and write up your solutions on your own.
- *Turn in .pdf file to Gradescope by the start of class on Tuesday, April 21, 2020.* It is simpler to put each problem on its own page using the LaTeX clearpage command.

Help Received:

- List any help received here, or "NONE".
  NONE

Exercises for Section 4.1:

38(a-d): (2 points).
we can calculate the remainder before we deal with the prime number.
a.
(361 mod 41) mod 9
= 33 mod 9
= 6
b.
$(216 mod 13)^2$ mod 11
= 64 mod 11
= 9
c.
$(343 mod 23)^2$ mod 31
= 21^2 mod 31
= 441 mod 31
= 7
d.
$(36 mod 15)^3$ mod 22
= 6^3 mod 22
= 216 mod 22
= 18

Exercises for Section 4.2:

Express the octal number 1437 in binary, decimal and hexadecimal: (1 point).
binary: 1100011111 decimal: 799 exadecimal: 31F

26: (2 points).
11^{644} mod 645
convert to binary first: a = 1010000100
there are ten digits, so: i = 0...9
x = 1
the base of power = 11
if a_n is not 1, simply square power then mod 645, and assign power with the result of it.
if a_n is 1, x times the previous power then x = x mod 645.
by the end of the calculation, x is the remainder we are looking for. 1. a1 = 0, x = 1, power = 121
2. a2 = 1, x = 1, power = 451
3. a3 = 0, x = 451, power = 121
4. a4 = 0, x = 451, power = 451
5. a5 = 0, x = 451, power = 226
6. a6 = 0, x = 451, power = 121
7. a7 = 1, x = 391, power = 451
8. a8 = 0, x = 391, power = 226
9. a9 = 1, x = 1

Exercises for Section 4.3:

24(a-b): (1 point).

a.

given that:

$a = 2^2 * 3^3 * 5^5$

$b = 2^5 * 3^3 * 5^2$

the common divider is the product of all the term with same base number but the smaller prime number.

thus the answer is $2^2 * 3^3 * 5^2 = 2700$

b.

with the same method, the answer is $2^1 * 3^1 * 11^1 = 66$

32(d-e): (2 points).

this method obtain the reminder by recursively getting the remainder of current numbers:

d.

14039 = 1529*9+278

1529 = 278*5+139

278 = 139*2

thus the remainder is 139

e.

with the same procedure:

14038 = 1529*9 + 277

1529 = 277*5 + 144

277 = 144*1+133

144 = 133*1 + 11

133 = 11*12 + 1

12 = 1*12

thus the answer is 1

40(d-e): (2 points).

we first apply the Euclidean algorithm, then build number back to the given numbers:

d.

55 = 2*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 remainder is 1, then build back:
= 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
= 2*8+(-3)*(13-1*8)
= 5*8+(-3)*13
= 5*(21-1*13) + (-3)*13
= 5*21+(-8)*13
= 5*21+(-8)*(55-2*21)
= 21*21 + (-8)*55

e. same procedure:
203 = 2*101 + 1
101 = 101 * 1
the remainder is 1
= 1
= 203 - 2* 101
= 1*203 + (-2) * 101

Exercises for Section 4.4:

6(a,c): (1 point).
to find the inverse, we first use the Euclidean algorithm:
17 = 8*2 + 1
2 = 2 * 1
thus the gcd is 1
then write them in terms of given numbers:
=1
=17-8*2
=1*17-8*2
the inverse is the coefficient of a, which is -8.
-8 mod 17 = 9 mod 17, so 9 is an alternative answer.

c.
first perform the Euclidean algorithm:
233 = 1*144+89
144 = 1*89 + 55
89 = 1*55 + 34
55 = 1*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
thus the gcd is 1
=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
=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*(55-1*34)-8*34
=13*55-21*34
=13*55-21*(89-1*55)
=34*55-21*89
=34*(144-1*89)-21*89
=34*144-55*89
=34*144-55*(233-1*144)
=89*144 - 55*233
the inverse of the coefficient of a, which is 89.

20: (2 points).
$a_1 = 1, a_2 = 2, a_3 = 3, a_4 = 4$
$n_1 = 2, n_2 = 3, n_3 = 5, n_4 = 11$
$n = n_1 * n_2 * n_3 * n_4 = 330$
$z_1 = n/n_1 = 165$
$z_2 = n/n_2 = 110$
$z_3 = n/n_3 = 66$
$z_4 = n/n_4 = 30$

$Y_1 = Z_1^{-1}(modn_1) \equiv 165^{-1}(mod2) \equiv 1^{-1}(mod2) \equiv 1(mod2) = 1$
$Y_2 = Z_2^{-1}(modn_2) \equiv 110^{-1}(mod3) \equiv 2^{-1}(mod3) \equiv 2(mod3) = 2$
$Y_3 = Z_3^{-1}(modn_3) \equiv 66^{-1}(mod5) \equiv 1^{-1}(mod5) \equiv 1(mod5) = 1$
$Y_4 = Z_4^{-1}(modn_4) \equiv 30^{-1}(mod11) \equiv 8^{-1}(mod11) \equiv 7(mod11) = 7$

$w_1 = Y_1 z_1(modn) \equiv 165(mod330) = 165$
$w_2 = Y_2 z_2(modn) \equiv 220(mod330) = 220$
$w_3 = Y_3 z_3(modn) \equiv 66(mod330) = 66$
$w_4 = Y_{44}(modn) \equiv 210(mod330) = 210$

$X \equiv a_1 w_1 + a_2 w_2 + ... + a_n w_n (mod(n))$
$X \equiv 1 * 165 + 2 * 220 + 3 * 66 + 4 * 210(mod(330))$
$X \equiv 1643(mod(330))$
$X = 323$
the general form is 323+330M, and M is arbitrary integer.

Exercises for Section 4.5:

4: (1 point).
since p=4969, there are 4969 spaces in the hash table.
find a space to store number with the first hashing function.
if the space is already occupied, use the second hashing function with the given initial number then plug back to the first function to find new space. increase i by 1 if the new space found is still occupied.
$h(k) = kmodp$
$g(k) = (k+1)mod(p-2)$
$h(k,i) = (h(k) + i * g(k))modp$
$k1 = 1524$
$k2 = 578$
$k3 = 2505$
$k4 = 2376$
$k5 = 3960$
$k6 = 1526$
$k7 = 2854$
$k8 = 4927$
$k9 = 1131$
$k10 = 4702$

20(a-d): (2 points).
for USPS code, the 11th digit is the remainder of sum of ten digits before then mod 9. **a)** $x_11 = x_1 + x_2 + ... + x_10 \mod 9$
$= Q + 1 + 2 + 2 + 3 + 1 + 3 + 9 + 7 + 8 \mod 9$
$= Q + 36 \mod 9$
$= (Q + (36 \mod 9) \mod 9$
$= Q \mod 9$
$Since x_11 = 4$
$Q \mod 9 = 4$
$Q = 4$
b) $x_11 = x_1 + x_2 + ... + x_10 \mod 9$
$= 6 + 7 + 0 + 2 + 1 + 2 + 0 + Q + 9 + 8 \mod 9$
$= Q + 35 \mod 9$
$= (Q + (35 \mod 9) \mod 9$
$= Q + 8 \mod 9$
$Since x_11 = 8$
$Q + 8 \mod 9 = 8$

$Q \mod 9 = 0$
$Q = 0 or Q = 9$
c) $x_1 1 = x_1 + x_2 + ... + x_1 0 \mod 9$
$= 2 + 7 + Q + 4 + 1 + 0 + 0 + 7 + 7 + 3 \mod 9$
$= Q + 31 \mod 9$
$= (Q + (31 \mod 9) \mod 9$
$= Q + 4 \mod 9$
$Since x_1 1 = 4$
$Q + 4 \mod 9 = 4$
$Q \mod 9 = 0$
$Q = 0$
d) $x_1 1 = x_1 + x_2 + ... + x_1 0 \mod 9$
$= 2 + 1 + 3 + 2 + 7 + 9 + 0 + 3 + 2 + Q \mod 9$
$= Q + 29 \mod 9$
$= (Q + (29 \mod 9) \mod 9$
$= Q + 2 \mod 9$
$Since x_1 1 = 1$
$Q + 2 \mod 9 = 1$
$Q \mod 9 = -1 \mod 9 = 8$
$Q = 8$

Exercises for Section 4.6:

8: (1 point).
Let A=0,B=1,C=2,...,Z=25
DVE CFMV KF NFEUVI REU KYRK ZJ KYV JVVU FW JTZVETV
= 3,21,4 2,5,12,21 10,5 13,5,4,20,21,8 17,4,20 10,24,17,10 25,9 10,24,21 9,21,21,20 5,22 9,19,25,21,4,19,21
the most common letter in ciphertext is V=21, and E=4 in English text
so k = 21- 4 = 17
$f^{-1}(P) = (P - 17) \mod 26$
12,4,13 11,14,21,4 19,14 22,14,13,3,4,17 0,13,3 19,7,0,19 8,18 19,7,4 18,4,4,3 14,5 18,2,8,4,13,2,4
= MEN LOVE TO WONDER AND THAT IS THE SEED OF SCIENCE
18: (1 point).
Let A=0,B=1,C=2,...,Z=25
Message = SNOWFALL = 18,13,14,22 5,0,11,11
Key = BLUE = 1,11,20,4
Applying encryption:
Message = 18+1,13+11,14+20,22+4 5+1,0+11,11+20,11+4 = 19,24,34,26 6,11,21,15
then take mod 26
19,24,8,0 6,11,5,15 = TYIA GLFP

26: (2 points).
first find d: d = 17 mod ((53-1)*(61-1)) = 2753
then decreypt each block using mapping
$M_1 = 3185^{2753} mod(3233) = 1816$
$M_2 = 2038^{2753} mod(3233) = 2008$
$M_3 = 2460^{2753} mod(3233) = 1717$
$M_4 = 2550^{2753} mod(3233) = 0411$
if A=00.. Z= 25, then the message is
SQ UI RR EL
which is squirrel.