CSCE 222 (Carlisle), Discrete Structures for Computing
Spring 2022
Homework 11

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.
HUY QUANG LAI

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 Monday, April 18, 2022.* It is simpler to put each problem on its own page using the LaTeX clearpage command.

Help Received:

- Rosen, Kenneth H. *Discrete Mathematics and Its Applications*. McGraw-Hill, 2019.

Exercises for Section 4.1:

38(a-d): (2 points).

Find each of these values.

a) $(19^2 \bmod 41) \bmod 9$
$= 2$

b) $(32^3 \bmod 13)^2 \bmod 11$
$= 9$

c) $(7^3 \bmod 23)^2 \bmod 31$
$= 7$

d) $(21^2 \bmod 15)^2 \bmod 22$
$= 14$

Exercises for Section 4.2:

Express the octal number 1437 in binary, decimal and hexadecimal: (1 point).

$1437_8 = 001100011111_2$
$1437_8 = 31F_{16}$
$1437_8 = 799_{10}$

26: (2 points).

Use Algorithm 5 to find $11^{644} \bmod 645$

$i = 0$: Because $a_0 = 0$, we have $x = 1$ and *power* $= 11^2 \bmod 645 = 11 \bmod 645 = 121$
$i = 1$: Because $a_1 = 0$, we have $x = 1$ and *power* $= 121^2 \bmod 645 = 14641 \bmod 645 = 451$
$i = 2$: Because $a_2 = 1$, we have $x = 1 \cdot 451 \bmod 645 = 451$ and *power* $= 451^2 \bmod 645 = 226$
$i = 3$: Because $a_3 = 0$, we have $x = 451$ and *power* $= 226^2 \bmod 645 = 121$
$i = 4$: Because $a_4 = 0$, we have $x = 451$ and *power* $= 121^2 \bmod 645 = 451$
$i = 5$: Because $a_5 = 0$, we have $x = 451$ and *power* $= 451^2 \bmod 645 = 226$
$i = 6$: Because $a_6 = 0$, we have $x = 451$ and *power* $= 226^2 \bmod 645 = 121$
$i = 7$: Because $a_7 = 1$, we have $x = 451 \cdot 121 \bmod 645 = 391$ and *power* $= 121^2 \bmod 645 = 451$
$i = 8$: Because $a_8 = 0$, we have $x = 391$ and *power* $= 451^2 \bmod 645 = 226$
$i = 9$: Because $a_9 = 1$, we have $x = 391 \cdot 226 \bmod 645 = 1$

Exercises for Section 4.3:

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

What are the greatest common divisors of these pairs of integers?

a) $2^2 \cdot 3^3 \cdot 5^5, 2^5 \cdot 3^3 \cdot 5^2$
$2^2 \cdot 3^3 \cdot 5^2$

b) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13, 2^{11} \cdot 3^9 \cdot 11 \cdot 17^{14}$
$2 \cdot 3 \cdot 11$

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

Use the Euclidean algorithm to find

d) $\gcd(1529, 14039)$

a:1529	b:14039
a:14039	b:1529
a:1529	b:278
a:278	b:139
a:139	b:0

$\gcd = 139$

e) $\gcd(1529, 14038)$

a:1529	b:14038
a:14038	b:1529
a:1529	b:277
a:277	b:144
a:144	b:133
a:133	b:11
a:11	b:1
a:1	b:0

$\gcd = 1$

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

Using the method followed in Example 17, express the greatest common divisor of each of these pairs of integers as a linear combination of these integers.

d) $21, 55$

$55 = 21 \cdot 2 + 13$
$21 = 13 \cdot 1 + 8$
$13 = 8 \cdot 1 + 5$
$8 = 5 \cdot 1 + 3$
$5 = 3 \cdot 1 + 2$
$3 = 2 \cdot 1 + 1$
$2 = 1 \cdot 2 + 0$

$1 = 3 - 1 \cdot 2$
$1 = 3 - 1 \cdot (5 - 3)$
$1 = 2 \cdot 3 - 1 \cdot 5$
$1 = 2 \cdot (8 - 1 \cdot 5) - 1 \cdot 5$
$1 = 2 \cdot 8 - 3 \cdot 5$
$1 = 2 \cdot 8 - 3 \cdot (13 - 1 \cdot 8)$
$1 = 5 \cdot (21 - 1 \cdot 13) - 3 \cdot 13$
$1 = 5 \cdot 21 - 8 \cdot 13$
$1 = 5 \cdot 21 - 8(55 - 2 \cdot 21)$
$1 = 21 \cdot 21 - 8 \cdot 55$

$\gcd(21, 55) = 1 = 21 \cdot 21 - 8 \cdot 55$

e) $101, 203$

$203 = 101 \cdot 2 + 1$
$101 = 1 \cdot 101 + 0$

$\gcd(101, 203) = 1 = 203 - 2 \cdot 101$

Exercises for Section 4.4:

6(a,c): (1 point).

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

a) $a = 2, m = 17$

$$17 = 8 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0$$

$1 = 17 - 8 \cdot 2$
$-8 \cdot 2 \bmod 17 = 1$
$9 \cdot 2 \bmod 17 = 1$
$\bar{a} = 9$

c) $a = 144, m = 233$

$$\begin{aligned} 233 &= 1 \cdot 144 + 89 \\ 144 &= 1 \cdot 89 + 55 \\ 89 &= 1 \cdot 55 + 34 \\ 55 &= 1 \cdot 34 + 21 \\ 34 &= 1 \cdot 21 + 13 \\ 21 &= 1 \cdot 13 + 8 \\ 13 &= 1 \cdot 8 + 5 \\ 8 &= 1 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \end{aligned}$$

20: (2 points).

Use the construction in the proof of the Chinese remainder theorem to find all solutions to the system of concurrences $x \equiv 2(\text{mod} 3), x \equiv 1(\text{mod} 4)$, and $x \equiv 3(\text{mod} 5)$.

$\text{lcm}(3, 4, 5) = 60$
$x = 2 \cdot 20 \cdot 20^{-1} \bmod 3 + 1 \cdot 15 \cdot 15^{-1} \bmod 4 + 3 \cdot 12 \cdot 12^{-1} \bmod 5$
$x = 2 \cdot 20 \cdot 2 + 1 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3$
$x = 233 \bmod 60$
$x = 53$

Exercises for Section 4.5:

4: (1 point).

Use the double hashing procedure we have described with $p = 4969$ to assign memory locations to files for employees with social security numbers $k_1 = 132489971, k_2 = 509496993,$
$k_3 = 546332190, k_4 = 034367980, k_5 = 047900151, k_6 = 329938157, k_7 = 212228844,$
$k_8 = 325510778, k_9 = 353354519, k_{10} = 053708912.$

$h(k) = k \bmod p$
$h(k_1) = 132489971 \bmod 4969$
$h(k_1) = 1524$

$h(k_2) = 509496993 \bmod 4969$
$h(k_2) = 578$

$h(k_3) = 546332190 \bmod 4969 = 578$
$g(k_3) = 546332191 \bmod 4967 = 1927$
$h(k, i) = (578 + 1(1927)) \bmod 4969 = 2505$

$h(k_4) = 034367980 \bmod 4969 = 2376$

$k_5 = 3960$
$k_6 = 1526$
$k_7 = 2854$
$k_8 = 4927$
$k_9 = 1131$
$k_{10} = 4702$

20(a-d): (2 points).

One digit in each of these identification numbers of a postal money order is smudged. Can you recover the smudged digit, indicated by a Q, in each of these numbers?

a) $Q1223139784$
$4 = (Q + 1 + 2 + 2 + 3 + 1 + 3 + 9 + 7 + 8) \bmod 9$
$4 = (Q + 36) \bmod 9$
$4 = Q \bmod 9$
$Q = 4$

b) $6702120Q988$
$8 = (6+7+0+2+1+2+0+Q+9+8) \bmod 9$
$8 = (Q+35) \bmod 9$
$8 = Q \bmod 9 + 8$
$0 = Q \bmod 9$
$Q = \{0, 9\}$

c) $27Q41007734$ $4 = (2+7+Q+4+1+0+0+7+7+3) \bmod 9$
$4 = (Q+31) \bmod 9$
$4 = Q \bmod 9 + 4$
$Q = \{0, 9\}$

d) $213279032Q1$
$1 = (2+1+3+2+7+9+0+3+2+Q) \bmod 9$
$1 = (Q+29) \bmod 9$
$-1 = Q \bmod 9$
$Q = 8$

Exercises for Section 4.6:

8: (1 point).

Suppose that the ciphertext DVE CFMV KF NFEUVI, REU KYRK ZJ KYV JVVU FW JTZVETV was produced by encrypting a plaintext message using a shift cipher. What is the original plaintext?

Shift 9 left or 17 right.
MEN LOVE TO WONDER, AND THAT IS THE SEED OF SCIENCE

18: (1 point).

Use the Vigenère cipher with key BLUE to encrypt the message SNOWFALL.

Key = BLUEBLUE
TYIACLFP

26: (2 points).

What is the original message encrypted using the RSA system with $n = 53 \cdot 61$ and $e = 17$ if the encrypted message is 3185 2038 2460 2550? (To decrypt, first find the decryption exponent d, which is the inverse of $e = 17 \bmod 52 \cdot 60$.)

$d = 2753$
$53 \cdot 61 = 3233$
$3185^d \bmod 3233 = 1816$
$2038^d \bmod 3233 = 2008$
$2460^d \bmod 3233 = 1717$
$2550^d \bmod 3233 = 0411$

$18, 16, 20, 08, 17, 17, 04, 11$
SQUIRREL