## Exercise 4.1

23 (a) Find a div m and a mod m when

(a) $a = 228, m = 119$

(b) $a = 9009, m = 223$

5(c) Find the integer a such that

(c) $a \equiv 99 \pmod{41}$ and $100 \leq a \leq 140$

## Exercise 4.2

7. Use Algorithm 5 to find $3^{2003} \bmod 99$

## Exercise 4.3

1) Determine whether each of these integers is prime

(e) 111

(f) 113

Que (3b) Find the prime factorization of each of these integers

(b) 126

(c) 729

7b Determine whether the integers in each of these sets are pairwise relatively prime. 14, 15, 21

29 Find $\gcd(92928, 123552) \cdot \operatorname{lcm}(92928, 123552) = 92928 \cdot 123552$ [Hint: First find the prime factorizations of 92928 and 123552.]

## Exercise 4.5

b Which memory locations are assigned by the hashing function $h(k) = k \bmod 97$ to the records of insurance company customers with these social security numbers 18321232

These last two congruences hold because $\sum_{i=1}^{10} x_i \equiv 0 \pmod{10}$ and $11 \nmid ja$, because $11 \nmid j$ and $11 \nmid a$. We conclude that $y_1 y_2 \ldots y_{10}$ is not a valid ISBN. So, we have detected the single error.

Now suppose that two unequal digits have been transposed. It follows that there are distinct integers $j$ and $k$ such that $y_j = x_k$ and $y_k = x_j$, and $y_i = x_i$ for $i \neq j$ and $i \neq k$. Hence,

$$\sum_{i=1}^{10} i y_i = \left(\sum_{i=1}^{10} i x_i\right) + (jx_k - jx_j) + (kx_j - kx_k) \equiv (j-k)(x_k - x_j) \not\equiv 0 \pmod{11},$$

because $\sum_{i=1}^{10} x_i \equiv 0 \pmod{10}$ and $11 \nmid (j-k)$ and $11 \nmid (x_k - x_j)$. We see that $y_1 y_2 \ldots y_{10}$ is not a valid ISBN. Thus, we can detect the interchange of two unequal digits.

## Exercises

1. Which memory locations are assigned by the hashing function $h(k) = k$ **mod** 97 to the records of insurance company customers with these Social Security numbers?
   a) 034567981 b) 183211232
   c) 220195744 d) 987255335

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) 104578690 b) 432222187
   c) 372201919 d) 501338753

3. A parking lot has 31 visitor spaces, numbered from 0 to 30. Visitors are assigned parking spaces using the hashing function $h(k) = k$ **mod** 31, where $k$ is the number formed from the first three digits on a visitor's license plate.
   a) Which spaces are assigned by the hashing function to cars that have these first three digits on their license plates: 317, 918, 007, 100, 111, 310?
   b) Describe a procedure visitors should follow to find a free parking space, when the space they are assigned is occupied.

Another way to resolve collisions in hashing is to use *double hashing*. We use an initial hashing function $h(k) = k$ **mod** $p$ where $p$ is prime. We also use a second hashing function $g(k) = (k+1)$ **mod** $(p-2)$. When a collision occurs, we use a *probing sequence* $h(k, i) = (h(k) + i \cdot g(k))$ **mod** $p$.

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

5. What sequence of pseudorandom numbers is generated using the linear congruential generator $x_{n+1} = (3x_n + 2)$ **mod** 13 with seed $x_0 = 1$?

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

7. What sequence of pseudorandom numbers is generated using the pure multiplicative generator $x_{n+1} = 3x_n$ **mod** 11 with seed $x_0 = 2$?

8. Write an algorithm in pseudocode for generating a sequence of pseudorandom numbers using a linear congruential generator.

The **middle-square method** for generating pseudorandom numbers begins with an $n$-digit integer. This number is squared, initial zeros are appended to ensure that the result has $2n$ digits, and its middle $n$ digits are used to form the next number in the sequence. This process is repeated to generate additional terms.

9. Find the first eight terms of the sequence of four-digit pseudorandom numbers generated by the middle square method starting with 2357.

10. Explain why both 3792 and 2916 would be bad choices for the initial term of a sequence of four-digit pseudorandom numbers generated by the middle square method.

The **power generator** is a method for generating pseudorandom numbers. To use the power generator, parameters $p$ and $d$ are specified, where $p$ is a prime, $d$ is a positive integer such that $p \nmid d$, and a seed $x_0$ is specified. The pseudorandom numbers $x_1, x_2, \ldots$ are generated using the recursive definition $x_{n+1} = x_n^d$ **mod** $p$.

11. Find the sequence of pseudorandom numbers generated by the power generator with $p = 7$, $d = 3$, and $x_0 = 2$.

12. Find the sequence of pseudorandom numbers generated by the power generator with $p = 11$, $d = 2$, and $x_0 = 3$.

13. Suppose you received these bit strings over a communications link, where the last bit is a parity check bit. For which string are you sure there is an error?
   a) 00000111111
   b) 10101010101
   c) 11111100000
   d) 10111101111

14. Prove that a parity check bit can detect an error in a string if and only if the string contains an odd number of errors.

The first nine digits of the ISBN-10 of the European version of the fifth edition of this book are 0-07-119881. What is the check digit for that book?

The ISBN-10 of the sixth edition of *Elementary Number Theory and Its Applications* is 0-321-500Q1-8, where $Q$ is a digit. Find the value of $Q$.

Determine whether the check digit of the ISBN-10 for this textbook (the seventh edition of *Discrete Mathematics and its Applications*) was computed correctly by the publisher.

United States Postal Service (USPS) sells money orders identified by an 11-digit number $x_1x_2 \ldots x_{11}$. The first ten digits identify the money order; $x_{11}$ is a check digit that satisfies $x_{11} = x_1 + x_2 + \cdots + x_{10} \bmod 9$.

Find the check digit for the USPS money orders that have identification number that start with these ten digits.

a) 7555618873
b) 6966133421
c) 8018927435
d) 3289744134

Determine whether each of these numbers is a valid USPS money order identification number.

a) 74051489623
b) 88382013445
c) 56152240784
d) 66606631178

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) $Q1223139784$
b) $6702120Q988$
c) $27Q41007734$
d) $213279032Q1$

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) $493212Q0688$
b) $850Q9103858$
c) $2Q941007734$
d) $66687Q03201$

Determine which single digit errors are detected by the USPS money order code.

Determine which transposition errors are detected by the USPS money order code.

Determine the check digit for the UPCs that have these initial 11 digits.

a) 73232184434
b) 63623991346
c) 04587320720
d) 93764323341

Determine whether each of the strings of 12 digits is a valid UPC code.

a) 036000291452
b) 012345678903
c) 782421843014
d) 726412175425

Does the check digit of a UPC code detect all single errors? Prove your answer or find a counterexample.

Determine which transposition errors the check digit of a UPC code finds.

Some airline tickets have a 15-digit identification number $a_1a_2 \ldots a_{15}$ where $a_{15}$ is a check digit that equals $a_1a_2 \ldots a_{14} \bmod 7$.

**28.** Find the check digit $a_{15}$ that follows each of these initial 14 digits of an airline ticket identification number.

a) 10237424413392
b) 00032781811234
c) 00611232134231
d) 00193222543435

**29.** Determine whether each of these 15-digit numbers is a valid airline ticket identification number.

a) 101333341789013
b) 007862342770445
c) 113273438882531
d) 000122347322871

**30.** Which errors in a single digit of a 15-digit airline ticket identification number can be detected?

***31.** Can the accidental transposition of two consecutive digits in an airline ticket identification number be detected using the check digit?

Periodicals are identified using an **International Standard Serial Number (ISSN)**. An ISSN consists of two blocks of four digits. The last digit in the second block is a check digit. This check digit is determined by the congruence $d_8 \equiv 3d_1 + 4d_2 + 5d_3 + 6d_4 + 7d_5 + 8d_6 + 9d_7 \pmod{11}$. When $d_8 \equiv 10 \pmod{11}$, we use the letter X to represent $d_8$ in the code.

**32.** For each of these initial seven digits of an ISSN, determine the check digit (which may be the letter X).

a) 1570-868
b) 1553-734
c) 1089-708
d) 1383-811

**33.** Are each of these eight-digit codes possible ISSNs? That is, do they end with a correct check digit?

a) 1059-1027
b) 0002-9890
c) 1530-8669
d) 1007-120X

**34.** Does the check digit of an ISSN detect every single error in an ISSN? Justify your answer with either a proof or a counterexample.

**35.** Does the check digit of an ISSN detect every error where two consecutive digits are accidentally interchanged? Justify your answer with either a proof or a counterexample.

Question 31

Alice wants to send to all her friends, including Bob, the message "SELL EVERYTHING" so that he knows that she sent it. What should she send to her friends, assuming she signs the message using the RSA cryptosystem?

## Exercises

1. Encrypt the message DO NOT PASS GO by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.
   a) $f(p) = (p + 3) \bmod 26$ (the Caesar cipher)
   b) $f(p) = (p + 13) \bmod 26$
   c) $f(p) = (3p + 7) \bmod 26$

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) $f(p) = (p + 4) \bmod 26$
   b) $f(p) = (p + 21) \bmod 26$
   c) $f(p) = (17p + 22) \bmod 26$

3. Encrypt the message WATCH YOUR STEP by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.
   a) $f(p) = (p + 14) \bmod 26$
   b) $f(p) = (14p + 21) \bmod 26$
   c) $f(p) = (-7p + 1) \bmod 26$

4. Decrypt these messages that were encrypted using the Caesar cipher.
   a) EOXH MHDQV
   b) WHVW WRGDB
   c) HDW GLP VXP

5. Decrypt these messages encrypted using the shift cipher $f(p) = (p + 10) \bmod 26$.
   a) CEBBOXNOB XYG
   b) LO WI PBSOXN
   c) DSWO PYB PEX

6. Suppose that when a long string of text is encrypted using a shift cipher $f(p) = (p + k) \bmod 26$, the most common letter in the ciphertext is X. What is the most likely value for $k$ assuming that the distribution of letters in the text is typical of English text?

7. Suppose that when a string of English text is encrypted using a shift cipher $f(p) = (p + k) \bmod 26$, the resulting ciphertext is DY CVOOZ ZOBMRKXMO DY NBOKW. What was the original plaintext string?

8. 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?

9. Suppose that the ciphertext ERC WYJJMGMIRXPC EHZERGIH XIGLRSPSKC MW MRHMWXMRKYMWLEFPI JVSQ QEKMG was produced by encrypting a plaintext message using a shift cipher. What is the original plaintext?

10. Determine whether there is a key for which the enciphering function for the shift cipher is the same as the deciphering function.

11. What is the decryption function for an affine cipher if the encryption function is $c = (15p + 13) \bmod 26$?

*12. Find all pairs of integers keys $(a, b)$ for affine ciphers for which the encryption function $c = (ap + b) \bmod 26$ is the same as the corresponding decryption function.

13. Suppose that the most common letter and the second most common letter in a long ciphertext produced by encrypting a plaintext using an affine cipher $f(p) = (ap + b) \bmod 26$ are Z and J, respectively. What are the most likely values of $a$ and $b$?

14. Encrypt the message GRIZZLY BEARS using blocks of five letters and the transposition cipher based on the permutation of $\{1, 2, 3, 4, 5\}$ with $\sigma(1) = 3$, $\sigma(2) = 5$, $\sigma(3) = 1$, $\sigma(4) = 2$, and $\sigma(5) = 4$. For this exercise, use the letter $X$ as many times as necessary to fill out the final block of fewer then five letters.

15. Decrypt the message EABW EFRO ATMR ASIN which is the ciphertext produced by encrypting a plaintext message using the transposition cipher with blocks of four letters and the permutation $\sigma$ of $\{1, 2, 3, 4\}$ defined by $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 4$, and $\sigma(4) = 2$.

*16. Suppose that you know that a ciphertext was produced by encrypting a plaintext message with a transposition cipher. How might you go about breaking it?

17. Suppose you have intercepted a ciphertext message and when you determine the frequencies of letters in this message, you find the frequencies are similar to the frequency of letters in English text. Which type of cipher do you suspect was used?

The **Vigenère cipher** is a block cipher, with a key that is a string of letters with numerical equivalents $k_1 k_2 \ldots k_m$, where $k_i \in \mathbf{Z}_{26}$ for $i = 1, 2, \ldots, m$. Suppose that the numerical equivalents of the letters of a plaintext block are $p_1 p_2 \ldots p_m$. The corresponding numerical ciphertext block is $(p_1 + k_1) \bmod 26 \, (p_2 + k_2) \bmod 26 \ldots (p_m + k_m) \bmod 26$. Finally, we translate back to letters. For example, suppose that the key string is RED, with numerical equivalents 17 4 3. Then, the plaintext ORANGE, with numerical equivalents 14 17 00 13 06 04, is encrypted by first splitting it into two blocks 14 17 00 and 13 06 04. Then, in each block we shift the first letter by 17, the second by 4, and the third by 3. We obtain 5 21 03 and 04 10 07. The cipherext is FVDEKH.

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

19. The ciphertext OIKYWVHBX was produced by encrypting a plaintext message using the Vigenère cipher with key HOT. What is the plaintext message?