Number Theory

Chapter 4

Edited by: Dr. Meshal Alfarhood

Applications of Congruences

Sections 4.5 and 4.6

Section Summary

Check Digits

- UPCs
- ISBNs

Cryptography

- Classical Cryptography
- Public Key Cryptography
  - RSA Cryptosystem

Check Digits: UPCs

- Retail products are identified by their ***Universal Product Codes*** (***UPCs***). Usually these have 12 decimal digits, the last one being the check digit. The check digit is determined by the congruence:

$$\mathbf{3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + x_8 + 3x_9 + x_{10} + 3x_{11} + x_{12} \equiv 0 \pmod{10}}$$

- **Examples**:

  a. If the first 11 digits of the UPC are 79357343104. What is the check digit?

  b. Is 041331021641 a valid UPC?

- **Solutions**:

  a. $3 \cdot 7 + 9 + 3 \cdot 3 + 5 + 3 \cdot 7 + 3 + 3 \cdot 4 + 3 + 3 \cdot 1 + 0 + 3 \cdot 4 + x_{12} \equiv 0 \pmod{10}$
  $21 + 9 + 9 + 5 + 21 + 3 + 12 + 3 + 3 + 0 + 12 + x_{12} \equiv 0 \pmod{10}$
  $98 + x_{12} \equiv 0 \pmod{10}$
  $\mathbf{x_{12} \equiv 2} \pmod{10}$ So, the check digit is **2**.

  b. $3 \cdot 0 + 4 + 3 \cdot 1 + 3 + 3 \cdot 3 + 1 + 3 \cdot 0 + 2 + 3 \cdot 1 + 6 + 3 \cdot 4 + 1 \equiv 0 \pmod{10}$
  $0 + 4 + 3 + 3 + 9 + 1 + 0 + 2 + 3 + 6 + 12 + 1 = 44 \equiv 4 \not\equiv 0 \pmod{10}$
  Hence, 041331021641 is **not** a valid UPC.

Check Digits: ISBNs

- **B**ooks are identified by an ***International Standard Book Number*** (**ISBN-10**), a 10 digit code. The first 9 digits identify the language, the publisher, and the book. The tenth digit is a check digit, which is determined by the following congruence:

$$x_{10} \equiv \sum_{i=1}^{9} i x_i \pmod{11}.$$

- The validity of an ISBN-10 number can be evaluated with: $\sum_{i=1}^{10} i x_i \equiv 0 \pmod{11}$

- **Examples:**

  a. Suppose that the first 9 digits of the ISBN-10 are 007288008. What is the check digit?

  b. Is 084930149X a valid ISBN10?

- **Solution**:

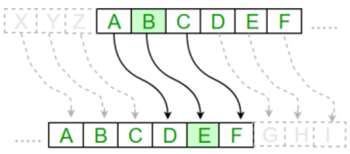
  a. $X_{10} \equiv 1 \cdot 0 + 2 \cdot 0 + 3 \cdot 7 + 4 \cdot 2 + 5 \cdot 8 + 6 \cdot 8 + 7 \cdot 0 + 8 \cdot 0 + 9 \cdot 8 \pmod{11}.$
  $X_{10} \equiv 0 + 0 + 21 + 8 + 40 + 48 + 0 + 0 + 72 \pmod{11}.$
  $X_{10} \equiv 189 \equiv 2 \pmod{11}$. Hence, $\boldsymbol{X_{10} = 2}$.

  b. $1 \cdot 0 + 2 \cdot 8 + 3 \cdot 4 + 4 \cdot 9 + 5 \cdot 3 + 6 \cdot 0 + 7 \cdot 1 + 8 \cdot 4 + 9 \cdot 9 + 10 \cdot 10 \equiv 0 \pmod{11}$
  $0 + 16 + 12 + 36 + 15 + 0 + 7 + 32 + 81 + 100 = 299 \equiv 2 \not\equiv 0 \pmod{11}$
  Hence, 084930149X is **not** a valid ISBN-10.

X is used for the digit 10.

Cryptography: Caesar Cipher

- Julius Caesar created secret messages by shifting each letter three letters forward in the alphabet.



- Here is how the encryption process works:
  - Replace each letter by an integer from $\mathbf{Z}_{26}$, that is an integer from 0 to 25.
  - The encryption function is $f(p) = (p + 3)$ **mod** 26.
  - Replace each new integer p back to alphabet letters.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

- **Example**: Encrypt the message "**MEET YOU IN THE PARK**" using Caesar cipher.
- **Solution**: 12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10.

  Now replace each of these numbers p by $f(p) = (p + 3)$ **mod** 26.

  15 7 7 22 1 17 23 11 16 22 10 7 18 3 20 13.

  Translating the numbers back to letters produces the encrypted message:

  "**PHHW BRX LQ WKH SDUN**"

Shift Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

- The Caesar cipher is one of a family of ciphers called *shift ciphers.* Letters can be shifted by an integer *k.*
- **Example**: Encrypt the message "**STOP GLOBAL WARMING**" using the shift cipher with $k = 11$.
- **Solution**:

18 19 14 15   6 11 14 1 0 11   22 0 17 12 8 13 6.

Apply the shift $f(p) = (p + 11)$ **mod** 26, yielding

3 4 25 0   17 22 25 12 11 22   7 11 2 23 19 24 17.

Translating the numbers back to letters produces the ciphertext

"**DEZA RWZMLW HLCXTYR**"

Public Key Cryptography

- All classical ciphers, including shift ciphers, are ***private key cryptosystems***. Knowing the encryption key allows one to quickly determine the decryption key.
  - All parties who wish to communicate using a private key cryptosystem must share the key and keep it a secret.
- In public key cryptosystems, knowing how to encrypt a message does not help one to decrypt the message. Therefore, everyone can have a publicly known <u>encryption key</u>. The only key that needs to be kept secret is the <u>decryption key</u>.

The RSA Cryptosystem

- **RSA** system was introduced in 1976 by three researchers at MIT.
- How does it work?
    1. Pick two large prime numbers, ***p*** and ***q***
    2. Let ***n*** = p x q
    3. Pick public key ***e*** $\ni \gcd\big(e, (p-1) \times (q-1)\big) = 1$
    4. Compute Secure key ***d*** $\ni \; de \equiv 1 \, mod \, ((p-1) \times (q-1))$.
- To <u>Encrypt</u>: $C = M^e \, mod(n)$, where M = original message and C = cipher text
- To <u>Decrypt</u>: $\mathrm{M} = C^{\mathrm{d}} \, mod(n)$

RSA Encryption

Example: Encrypt the message "STOP" using the RSA cryptosystem.

- Let p = 43, q = 59.
- n = 43 · 59 = 2537.
- Pick e=13, where gcd(13, 42 · 58) = 1 → gcd(13, 2436) = 1
- Compute $\boldsymbol{d} \ni\ 13d \equiv 1\ mod(2436)$.
  - Using Extended Euclidean, we get (937 x 13 – 5 x 2436) =1 → d=937
- Translate the letters in "STOP" to their numerical equivalents 18 19 14 15.
- Divide into blocks of four digits to obtain 1819 1415.
- Encrypt each block using the mapping $C = M^{13}$ **mod** 2537.
- $C_1 = 1819^{13}$ **mod** 2537 = 2081
- $C_2 = 1415^{13}$ **mod** 2537 = 2182
- The encrypted message is 2081 2182.
- To decrypt the message:
  - $M_1 = 2081^{937}$ **mod** 2537 = 1819
  - $M_2 = 2182^{937}$ **mod** 2537 = 1415