Applications of number theory

Letter-to-number conversion

Throughout this tipsheet, we use the standard mapping:

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

Caesar ciphers

A **Caesar cipher** encrypts a message by shifting each letter by a fixed amount. The general form is:

$$f(k) = (ak + b) \mod 26$$

where k is the numerical value of the plaintext letter, and $f(k)$ is the numerical value of the ciphertext letter.
The classic Caesar cipher uses $a = 1$ and $b = 3$, giving $f(k) = (k + 3) \mod 26$.

Encryption

Steps:

1. Convert each letter to its number (A = 0, B = 1, ..., Z = 25)
2. Apply the encryption function $f(k) = (ak + b) \mod 26$
3. Convert the result back to a letter

Example: Encrypt "EUCLIDEAN" using $f(k) = (5 + 8k) \mod 26$.

Letter	E	U	C	L	I	D	E	A	N
k	4	20	2	11	8	3	4	0	13
$5 + 8k$	37	165	21	93	69	29	37	5	109
$f(k) = (5 + 8k) \mod 26$	11	9	21	15	17	3	11	5	5
Ciphertext	L	J	V	P	R	D	L	F	F

The encrypted message is **LJVPRDLFF**.

Student Learning Support, Teaching and Learning Centre
studentlearning@ontariotechu.ca
ontariotechu.ca/studentlearning

OntarioTech UNIVERSITY

Decryption

To decrypt, find the inverse function. If $f(k) = (ak + b) \mod 26$, then:

$$f^{-1}(c) = a^{-1}(c - b) \mod 26$$

where a^{-1} is the multiplicative inverse of a modulo 26.
Note: For the inverse to exist, $\gcd(a, 26) = 1$.

Linear congruential generators

A **linear congruential generator** (LCG) produces a sequence of pseudorandom numbers using:

$$x_{n+1} = (ax_n + c) \mod m$$

Parameter	Name
m	Modulus
a	Multiplier
c	Increment
x_0	Seed (starting value)

Example: Generate pseudorandom numbers with $m = 13$, $a = 3$, $c = 2$, $x_0 = 1$.
Apply $x_{n+1} = (3x_n + 2) \mod 13$ repeatedly:

n	x_n	$3x_n + 2$	$x_{n+1} = (3x_n + 2) \mod 13$
0	1	5	5
1	5	17	4
2	4	14	1
3	1	5	5

The sequence is: $1, 5, 4, 1, 5, 4, 1, \ldots$ (repeats with period 3)
Note: The sequence will eventually repeat. The maximum possible period is m. Good parameter choices maximize the period.
Example: Generate pseudorandom numbers with $m = 9$, $a = 7$, $c = 4$, $x_0 = 3$.

n	x_n	$7x_n + 4$	$x_{n+1} = (7x_n + 4) \mod 9$
0	3	25	7
1	7	53	8
2	8	60	6
3	6	46	1
4	1	11	2
5	2	18	0
6	0	4	4
7	4	32	5
8	5	39	3
9	3	25	7

The sequence is: $3, 7, 8, 6, 1, 2, 0, 4, 5, 3, \ldots$ (full period of 9)

Check digits

Check digits detect errors in identification numbers using modular arithmetic.

ISBN-10

An ISBN-10 has the form $x_1x_2x_3x_4x_5x_6x_7x_8x_9x_{10}$ where x_{10} is the check digit.
Check digit formula:

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

or equivalently, a valid ISBN-10 satisfies:

$$\sum_{i=1}^{10} i \cdot x_i \equiv 0 \pmod{11}$$

Note: If the check digit is 10, it is written as X.
Example: Find the check digit for ISBN 0-13-110362-?

$$\sum_{i=1}^{9} i \cdot x_i = 1(0) + 2(1) + 3(3) + 4(1) + 5(1) + 6(0) + 7(3) + 8(6) + 9(2)$$
$$= 0 + 2 + 9 + 4 + 5 + 0 + 21 + 48 + 18 = 107$$

$x_{10} \equiv -107 \equiv -107 + 110 \equiv 3 \pmod{11}$
The check digit is **3**, so the ISBN is 0-13-110362-3.

ISBN-13

An ISBN-13 has the form $x_1x_2 \ldots x_{13}$ where x_{13} is the check digit.

Check digit formula:

$$x_{13} \equiv -\sum_{i=1}^{12} w_i \cdot x_i \pmod{10}$$

where weights alternate: $w_i = 1$ if i is odd, $w_i = 3$ if i is even.

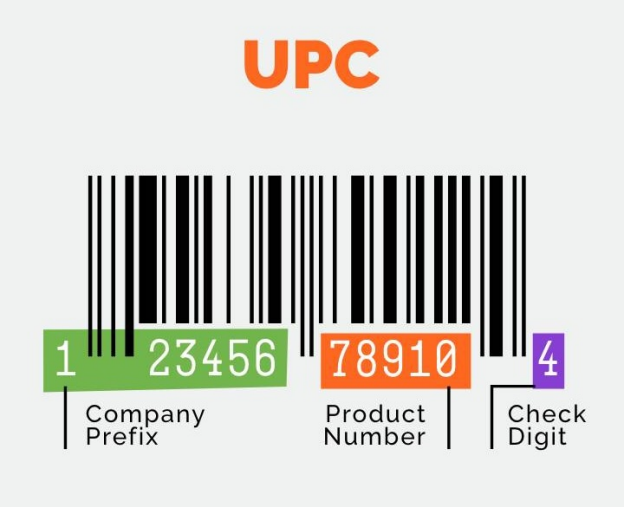
Example: Find the check digit for ISBN 978-0-13-213080-?

$$\begin{aligned} &1(9) + 3(7) + 1(8) + 3(0) + 1(1) + 3(3) + 1(2) + 3(1) + 1(3) + 3(0) + 1(8) + 3(0) \\ &= 9 + 21 + 8 + 0 + 1 + 9 + 2 + 3 + 3 + 0 + 8 + 0 = 64 \end{aligned}$$

$x_{13} \equiv -64 \equiv -64 + 70 \equiv 6 \pmod{10}$

The check digit is **6**.

UPC-A



A UPC-A has 12 digits: $x_1 x_2 \ldots x_{12}$ where x_{12} is the check digit.

Check digit formula:

$$x_{12} \equiv -\sum_{i=1}^{11} w_i \cdot x_i \pmod{10}$$

where $w_i = 3$ if i is odd, $w_i = 1$ if i is even.

Note: UPC uses the opposite weighting pattern from ISBN-13!

Example: Find the check digit for UPC 07385003284?

$$\begin{aligned} &3(0) + 1(7) + 3(3) + 1(8) + 3(5) + 1(0) + 3(0) + 1(3) + 3(2) + 1(8) + 3(4) \\ &= 0 + 7 + 9 + 8 + 15 + 0 + 0 + 3 + 6 + 8 + 12 = 68 \end{aligned}$$

$x_{12} \equiv -68 \equiv -68 + 70 \equiv 2 \pmod{10}$

Student Learning Support, Teaching and Learning Centre
studentlearning@ontariotechu.ca
ontariotechu.ca/studentlearning

The check digit is **2**.

Quick reference

Application	Formula	Key detail
Caesar cipher	$f(k) = (ak + b) \mod 26$	Need $\gcd(a, 26) = 1$
LCG	$x_{n+1} = (ax_n + c) \mod m$	Sequence repeats
ISBN-10	$\sum_{i=1}^{10} i \cdot x_i \equiv 0 \pmod{11}$	Check digit can be X
ISBN-13	Weights: $1, 3, 1, 3, \ldots \pmod{10}$	Starts with 978 or 979
UPC-A	Weights: $3, 1, 3, 1, \ldots \pmod{10}$	Opposite of ISBN-13

Student Learning Support, Teaching and Learning Centre
studentlearning@ontariotechu.ca
ontariotechu.ca/studentlearning