

MA180, MA185, MA190

Algebra & Calculus
Graham Ellis

Algebra

Topics

- Elementary number theory

- Matrix theory

- Eigenvectors & Eigenvalues

Context

Internet communications

Geometry & Internet communications

Breeding rabbits

Elementary Number Theory

$$5 + 15 = 20$$

in school

$$7 + 10 = 5$$

on a clock

$$7 + 10 \equiv 5 \pmod{12}$$

Today is Monday. In 73 days time it will be Thursday.

$$1 + 73 \equiv 4 \pmod{7}$$

More examples

$$10 \times 5 \equiv 2 \pmod{12}$$

$$7 + 5 \equiv 3 \pmod{9}$$

$$7 \times 8 \equiv 2 \pmod{9}$$

$$2 - 5 \equiv 5 \pmod{8}$$

What is $\frac{1}{3}$?

What is $1 \div 3$?

$\frac{1}{3}$ is that number with the property

$$\left(\frac{1}{3}\right) \times 3 = 1$$

Alternative notation

$$3^{-1} = \frac{1}{3}$$

We call 3^{-1} the inverse of 3.

Back to clocks

What is $7^{-1} \pmod{10}$?

$$\boxed{7^{-1} \equiv 3 \pmod{10}}$$

because $7 \times 3 \equiv 1 \pmod{10}$

Applications

Any book is identified by an ISBN. On older books this is a string of 10 digits.

0 5 5 2 1 2 4 7 5 3

Terry Pratchett

The final digit is a safety check digit. It is chosen so that

$$\begin{aligned}
 & (1 \times 0) + (2 \times 5) + (3 \times 5) + (4 \times 2) + (5 \times 1) \\
 & + (6 \times 2) + (7 \times 4) + (8 \times 7) + \\
 & (9 \times 5) + (10 \times 3)
 \end{aligned}$$

$$\begin{aligned}
 \equiv & 0 + 1 + 4 + 3 + 5 + 1 + 6 \quad \text{mod } 11 \\
 & + 1 + 1 + 8
 \end{aligned}$$

$$\equiv 0 \quad \text{mod } 11$$

Second Example

$$0 \ 1 \ 4 \ y \ 2 \ 2 \ 5 \ 8 \ 9 \ 7$$

$$\begin{aligned}
 & 1 \cdot 0 + 2 \cdot 1 + 3 \cdot 4 + 4 \cdot y + 5 \cdot 2 + 6 \cdot 2 \\
 & + 7 \cdot 5 + 8 \cdot 8 + 9 \cdot 9 + 10 \cdot 7
 \end{aligned}$$

$$\begin{aligned}
 \equiv & 2 + 1 + 4y + 1 + 1 + 2 + 2 \quad \text{mod } 11 \\
 & + 4 + 4
 \end{aligned}$$

$$\equiv 0 + 4y \quad \text{mod } 11$$

Hence $y = 0$.