

MA180, MA185, MA190 Welcome

MA161, MA133, MA160 Not Welcome

Algebra & Calculus

Graham Ellis

Algebra

Topics

- Elementary number theory

- matrix theory

- Eigenvalues & Eigenvectors

Context

Internet communications

Geometry & internet communication

Breeding rabbits

# Elementary Number Theory

$$5 + 15 = 20$$

in school

$$9 + 11 = 8$$

on a clock

$$9 + 11 \equiv 8 \pmod{12}$$

Today is Monday. In 73 days time it will be

Thursday

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

More Examples

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

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

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

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

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 multiplicative inverse of 3.

## Back to Clocks

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

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

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

## Applications

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

0 7 0 4 3 3 1 6 5 9

*The Durb*

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

$$(1 \times 0) + (2 + 7) + (3 + 0) + (4 + 4) + (5 + 3) \\ + (6 \times 3) + (7 + 1) + (8 \times 6) + (9 + 5) \\ + (10 \times 4)$$

$$\equiv 0 + 3 + 0 + 5 + 4 + 7 + 7 \\ + 4 + 1 + 2$$

$$\equiv 11$$

$$\equiv 0 \pmod{11}$$

---

Second Example

0 1 9 9 2 9 7 4 1 9

$$\begin{aligned}
 &1 \cdot 0 + 2 \cdot 1 + 3 \cdot 9 + 4 \cdot 9 + 5 \cdot 2 \\
 &+ 6 \cdot y + 7 \cdot 7 + 8 \cdot 4 + 9 \cdot 1 + 10 \cdot 9 \\
 &\equiv 0 \pmod{11}
 \end{aligned}$$

$$\begin{aligned}
 &\cancel{1} + 5 + 3 - \cancel{1} + 6y + 5 \\
 &\cancel{-1} - \cancel{2} + \cancel{2} \equiv 0
 \end{aligned}$$

$$-2 = 6y$$

$$y = -6^{-1} \cdot 2$$

$$6^{-1} \equiv 2 \pmod{11}$$

$$y = -2 \cdot 2 = -4 \equiv 7$$