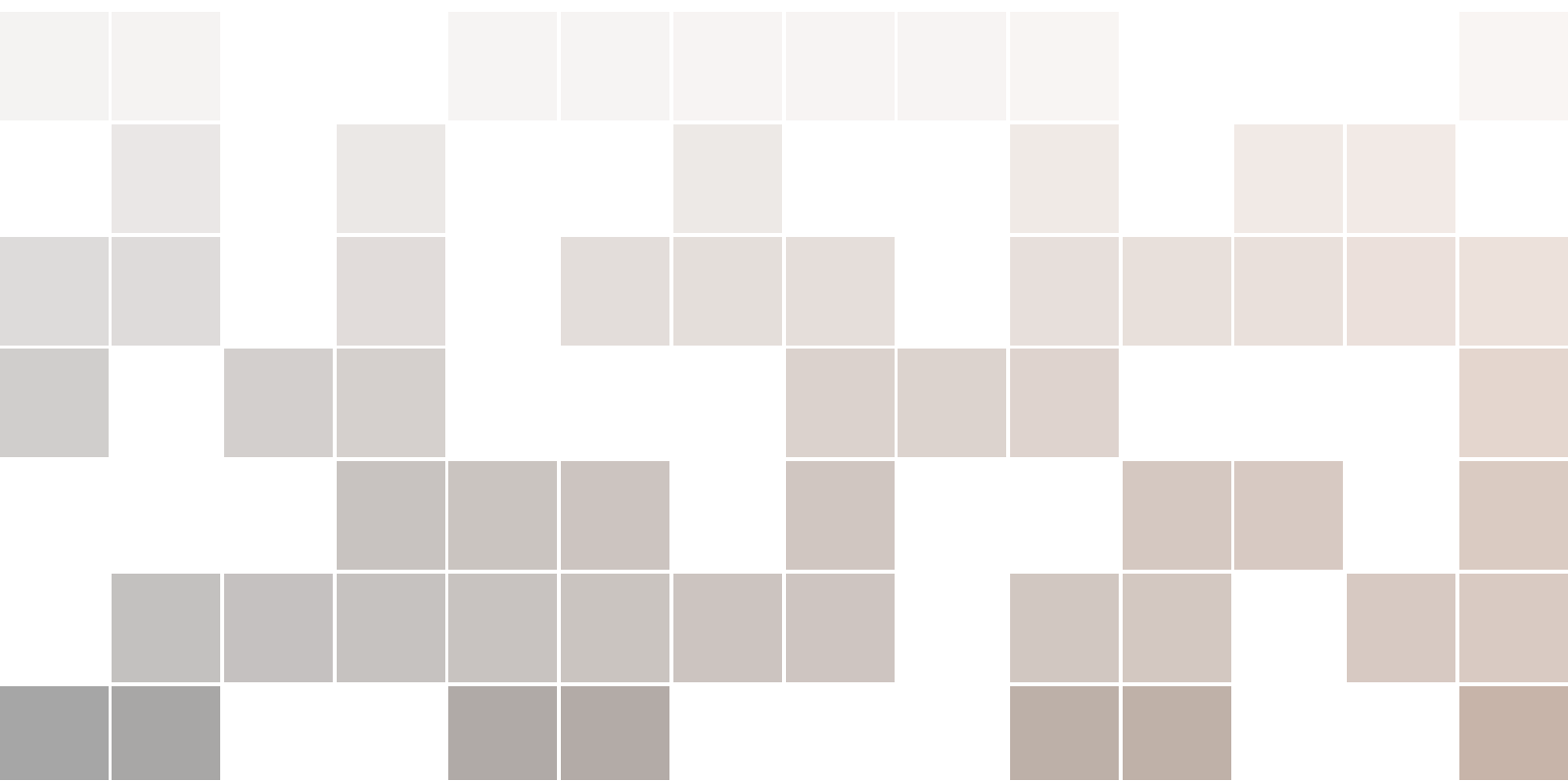


A short introduction to university algebra

22 lectures for online study during Covid-19

Graham Ellis



Copyright © 2020 Graham Ellis

PUBLISHED BY *Shoe String Press*

[HTTP://HAMILTON.NUIGALWAY.IE](http://HAMILTON.NUIGALWAY.IE)

Licensed under the Creative Commons Attribution-NonCommercial 3.0 Unported License (the “License”). You may not use this file except in compliance with the License. You may obtain a copy of the License at <http://creativecommons.org/licenses/by-nc/3.0>. Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

First release, October-December 2020

Contents

I	Arithmetic	
1	Basic arithmetic	9
1.1	Addition	10
1.2	Subtraction	10
1.3	Multiplication	11
1.4	Division	11
1.5	Is there any point to all this?	11
2	Euclid's algorithm and bank accounts	13
2.1	Euclidean algorithm	13
2.2	Bézout's identity	14
2.3	Inverses in clock arithmetic	15
2.4	Bank account numbers	15
3	War, finance and arithmetic	17
3.1	Basic assumptions	18
3.2	A first mathematical example	18
4	Cryptography and arithmetic	21
4.1	A lesson to be learned	22

5	An old Chinese theorem	25
5.1	Variant of the classical puzzles	26
5.2	Extracting a theorem	27
6	Euler Phi Function and digital signatures	29
6.1	What is a proposition?	29
6.2	Two more propositions	30
6.3	Public Key Cryptography	31
6.4	Digital signatures	32
6.5	A puzzle	32
7	Calculation of powers	35
7.1	Euler's theorem	36
7.2	Fermat's little theorem	36
7.3	In readiness for RSA cryptography	37
8	Pretty good privacy	39
8.1	RSA cryptosystem	40
8.2	Two remarks	41

II

Matrices

9	Basic arithmetic	45
9.1	Matrices	45
9.2	Matrix addition	45
9.3	Multiplication of a column vector by row vector	46
9.4	Matrix multiplication	47
9.5	Algebraic properties	47
10	Scalars, division, affine cryptography	49
10.1	Algebraic properties of scalar multiplication	49
10.2	Identity matrices	49
10.3	Inverse matrices	50
10.4	Affine cryptography	51
10.5	A puzzle	53
11	A cyber attack	55
11.1	A secure cryptosystem in inexperienced hands	56
12	Linear transformations of the plane	59
12.1	Algebra versus Geometry	59
12.2	Linear transformations	61

12.3	Transformations that preserve lines	64
13	Geometry of matrices	65
13.1	Why did that proof work?	67
13.2	Matrix multiplication explained	68
13.3	Rotations and reflections	68
14	Inverse matrices	71
15	Row operations	73
16	Determinants	75

III	Eigenvalues
------------	--------------------

17	Eigenvalues and eigenvectors	79
18	Google search engine	81
19	Calculating eigenvalues and eigenvectors	83
20	The Golden Ratio	85
21	More on the Golden Ratio	87
22	A Model of infectious diseases	89
	Bibliography	91
	Articles	91
	Books	91



Arithmetic

1	Basic arithmetic	9
1.1	Addition	
1.2	Subtraction	
1.3	Multiplication	
1.4	Division	
1.5	Is there any point to all this?	
2	Euclid's algorithm and bank accounts	13
2.1	Euclidean algorithm	
2.2	Bézout's identity	
2.3	Inverses in clock arithmetic	
2.4	Bank account numbers	
3	War, finance and arithmetic	17
3.1	Basic assumptions	
3.2	A first mathematical example	
4	Cryptography and arithmetic	21
4.1	A lesson to be learned	
5	An old Chinese theorem	25
5.1	Variant of the classical puzzles	
5.2	Extracting a theorem	
6	Euler Phi Function and digital signatures	29
6.1	What is a proposition?	
6.2	Two more propositions	
6.3	Public Key Cryptography	
6.4	Digital signatures	
6.5	A puzzle	
7	Calculation of powers	35
7.1	Euler's theorem	
7.2	Fermat's little theorem	
7.3	In readiness for RSA cryptography	
8	Pretty good privacy	39
8.1	RSA cryptosystem	
8.2	Two remarks	

1. Basic arithmetic

What might we say about the following four equations?

$$5 + 4 = 9 \tag{1.1}$$

$$10 + 11 = 9 \tag{1.2}$$

$$298 + 71 = 9 \tag{1.3}$$

$$9 = 9 \tag{1.4}$$

We might be inclined to say the first is correct, the second and third are incorrect, and the last is obvious. Certainly, if Jessie has a basket of 5 apples, and she adds 4 apples to it, then she'll have a basket of 9 apples. If she has a basket of 10 apples, and adds 11 more to it, then she'll not have a basket of 9 apples. On the other hand, if Mary starts work at 10 o'clock, and she works for 11 hours, then she'll finish work at 9 o'clock. If Joseph is sailing on a course of 298° , and he decides to add 71° to his course, then he'll be on a course of 9° . So statements (1.2) and (1.3) can be true, and it's a bit rash to declare them outright incorrect..

Maybe it is safer to say that equation (1.1) is always true, equations (1.2) and (1.3) can be true or false depending on their context, and equation (1.4) is obviously true. But what exactly does equation (1.1) mean? Does it mean that $5 + 4$ is indistinguishable from 9 and that we lose no information when we replace the symbols $5 + 4$ by the symbol 9? If it meant that, then equation (1.1) and (1.4) would be the same equation. But they are clearly not the same equation as $9 = 9$ has always been obvious to us, yet we had to spend months in primary school learning that $5 + 4 = 9$.

Conclusion. After all our years in school we still don't really know what $5 + 4 = 9$ means, and we are unable to decide whether the equation $10 + 11 = 9$ is true or false.

The equations

$$10 + 11 = 9 \text{ on a 12-hour clock} \tag{1.5}$$

$$298 + 71 = 9 \text{ on a 360-degree compass} \tag{1.6}$$

are correct, as are

$$10 + 11 = 9 \quad \text{on a 12-month calendar} \quad (1.7)$$

$$298 + 71 = 9 \quad \text{on the 360-day calendar used in finance.} \quad (1.8)$$

It is convenient to introduce a notation and vocabulary that allows us to treat equations (1.5) and (1.7) as being essentially the same equation. The notation we use is:

$$10 + 11 \equiv 9 \pmod{12} \quad (1.9)$$

The vocabulary we use is:

$$10 + 11 \text{ is congruent to } 9 \text{ modulo } 12 \quad (1.10)$$

We might also write

$$10 + 11 \not\equiv 8 \pmod{12} \quad (1.11)$$

and say

$$10 + 11 \text{ is not congruent to } 8 \text{ modulo } 12. \quad (1.12)$$

All of the above discussion is summarized in the following.

Definition 1.0.1 For integers a, b, c, m we write

$$a + b \equiv c \pmod{m} \quad (1.13)$$

to mean that $(a + b) - c$ is an integer multiple of m .

1.1 Addition

We are now in a position to make calculations such as the following.

$$13 + 15 \equiv 4 \pmod{24} \quad (1.14)$$

$$13 + 15 \not\equiv 4 \pmod{23} \quad (1.15)$$

$$13 + 15 \equiv 5 \pmod{23} \quad (1.16)$$

$$7 + 23 \equiv 7 \pmod{23} \quad (1.17)$$

$$23 \equiv 0 \pmod{23} \quad (1.18)$$

$$7 + 16 \equiv 0 \pmod{23} \quad (1.19)$$

1.2 Subtraction

In light of equation (1.19) we write:

$$-7 \equiv 16 \pmod{23} \quad (1.20)$$

One way to understand equation (1.20) is to note that it refers to an arithmetic calculation on a 23-hour clock, and that on such a clock there are only twenty-three numbers, namely the numbers $0, 1, 2, \dots, 22$. So for instance, we don't allow 25 as an answer to any calculation in this context as it doesn't appear on a 23-hour clock, but we do allow 2 and note that the equation

$$25 \equiv 2 \pmod{23} \quad (1.21)$$

holds. So in place of 25 we write 2. Now -7 does not appear on a 23-hour clock, so what should we write in place of it? Well whatever -7 is, it should satisfy:

$$7 + (-7) \equiv 0 \pmod{23} \quad (1.22)$$

In other words, -7 should be a number on the clock which, when added to 7, yields the answer 0. Equation (1.19) tells us that 16 is such a number. A little experimentation shows that 16 is the only such number. Hence we arrive at (1.20).

We are now in a position to make the following calculations.

$$37 + (-8) \equiv 3 \pmod{26} \quad (1.23)$$

$$5 + 8 \equiv -4 \pmod{9} \quad (1.24)$$

$$5 - 8 \equiv 6 \pmod{9} \quad (1.25)$$

1.3 Multiplication

Multiplication on a clock is no problem. For instance:

$$7 \times 8 \equiv 6 \pmod{10} \quad (1.26)$$

$$7 \times (-8) \equiv 4 \pmod{10} \quad (1.27)$$

$$5 \times 13 \equiv 1 \pmod{16} \quad (1.28)$$

1.4 Division

What should we mean by 5^{-1} on a 16-hour clock? The most reasonable interpretation is that the multiplicative inverse of 5 should be one of the numbers on the clock which, when multiplied by 5, yields 1. Equation (1.28) shows that 13 is one such number, and a bit of experimentation establishes that this is the only such number on the clock. So we write:

$$5^{-1} \equiv 13 \pmod{16} \quad (1.29)$$

1.5 Is there any point to all this?

Clock arithmetic is used quite a lot. As one example, suppose we wanted to order the book

The Famous Five - Five on a Treasure Island by Enid Blyton

from the University library. We would simply send the book's 10-digit International Standard Book Number (ISBN) 034-002-423-2 to the library acquisitions office. In fact, any (older) book is uniquely identified by the first nine digits of its ISBN. So we could actually just send the acquisitions office the number 034-002-423, and we would receive the book. Well, we'd receive the book assuming that the librarian forwarded our nine digits correctly. Humans are prone to making mistakes. The librarian might get one of the nine digits wrong, say the last one, and forward 034-002-421 which uniquely identifies the book

Shadows by Donald Hamilton

about a political maniac with a scheme to shadow and kill prominent public figures in a takeover plot and who can only be stopped by using a beautiful woman as bait. The reason for the tenth digit is that a publisher would immediately know that the 10-digit number 034-002-421-2 is not a valid ISBN number and would ask the library for correct information before sending out any book.

The last digit of a 10-digit ISBN $x_1x_2x_3\dots x_{10}$ is chosen so that the equation

$$x_1 + 2x_2 + 3x_3 + \dots + 10x_{10} \equiv 0 \pmod{11} \quad (1.30)$$

holds. If this equation does not hold then the 10-digit number is not a valid ISBN and must contain an error. The final digit can be computed from the first nine digits using the formula

$$x_{10} \equiv -10^{-1}(x_1 + 2x_2 + 3x_3 + \dots + 9x_9) \pmod{11} \quad (1.31)$$

on an 11-hour clock. If $x_{10} \equiv 10 \pmod{11}$ then it is represented by the symbol X in the ISBN.

We can calculate the check digit x_{10} for the *Shadows* book as follows.

$$\begin{aligned} x_{10} &\equiv -10^{-1}(1 \times 0 + 2 \times 3 + 3 \times 4 + 4 \times 0 + 5 \times 0 + 6 \times 2 + 7 \times 4 + 8 \times 2 + 9 \times 1) && \pmod{11} \\ &\equiv -10(6 + 12 + 12 + 28 + 16 + 9) && \pmod{11} \\ &\equiv (6 + 1 + 1 + 6 + 5 + 9) && \pmod{11} \\ &\equiv 28 && \pmod{11} \\ &\equiv 6 && \pmod{11} \end{aligned}$$