M 2 4 6

Number Theory

Workbook 0 (with solutions)

Fundamental Properties of the Integers
(Revision of material from Foundations)

Summer 2013

(originally written and devised by
Trevor Hawkes and Alyson Stibbard;
revised in 2010 by John Cremona)

Aims of this workbook:

(a) To give you the flavour of learning mathematics through directed problem solving in this workbook format. The course will be taught through five such workbooks.

(b) To help you to revise the material covered (or hinted at) in "Foundations". Such material forms the starting point for this course in Number Theory.

(c) To summarise the key ideas that underlie the so-called Fundamental Theorem of Arithmetic.

(d) To enable you thereby to decide whether you want to take this course.

Copies of this workbook, both with and without solutions, can be found on Mathstuff.

In this course you will constantly get your hands dirty and, I hope, your brain engaged. You will be expected to calculate, to experiment, and to explore, in order to uncover some of the secrets of the counting numbers 1,2,3,.. that have fascinated our ancestors since the dawn of history.

Note: You will need a pocket calculator for some of the questions in the workbooks, and are encouraged to use one for this purpose and to experiment with results and ideas in the course. Calculators are NOT needed and are NOT allowed in tests or in the examination.

These workbooks were orginally written and devised by *Trevor Hawkes and and Alyson Stibbard*. *Ben Carr* designed the LaTeX template and *Rob Reid* converted their drafts into elegant print. Over the years, other lecturers and students have corrected a number of typos, mistakes and other infelicities. In 2010 *John Cremona* made some substantial revisions.

Send corrections, ask questions or make comments at the module forum. You can join the MA246 forum by going to `http://forums.warwick.ac.uk/wf/misc/welcome.jsp` and signing in, clicking the *browse* tab, and then following the path: Departments > Maths > Modules > MA2xx modules > MA246 Number Theory.

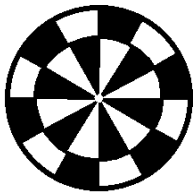
1 Divisors and Units

Section Targets

(a) To explore the concept of **division** for integers.

(b) To understand the special role of elements which divide 1.

(c) To understand the special role of elements which divide 0.



We are very precise about the meaning of the word *divides*. If in doubt always refer back to this definition.

(1.1) Definition Let a and b be integers. We say b *divides* a (and write $b|a$) if there exists an integer c such that

$$a = bc. \tag{1.a}$$

We call b a *divisor* or a *factor* of a.

Notice that you get a very different answer to these questions if b and c are allowed to be rational numbers.

(1.2) Questions about Definition 1.1
What are the possible values for the integers b and c in Equation 1.a:

(a) when $a = 0$?

(b) when $a = 1$?

The numbers 0 and 1 play a special role in the study of division. The numbers that divide 1 get a special name; they are called *units*.

(1.3) Questions about divisors.

(a) Which integers divide 0 ?

(b) Which integers are divisible by 0 ?

(c) Which integers divide 1 ?

(d) Which integers are divisible by 1 ?

Although zero divides zero, no meaning is given to the quotient

$$\frac{0}{0}.$$

Answers to (1.3)

(a) For every integer b, $0 = b \times 0$. Hence every integer divides 0.

(b) To say $0|a$ means there exists an integer c such that $a = 0 \times c = 0$. Hence, 0 is the only integer divisible by 0.

(c) If b divides 1, then $bc = 1$ for some $c \in \mathbb{Z}$. The only possibilities are $b = c = 1$ and $b = c = -1$.

(d) Since $a = 1 \times a$, **all** integers are divisible by 1.

(1.4) Definition We call an element u a **unit** if there exists an element v such that $uv = 1$. Thus a unit is simply an element which divides 1.

A non-zero element a for which another *non-zero* element b exists with $ab = 0$ is called a **zero divisor**. Thus $\mathbb{Z}/4\mathbb{Z}$ has zero divisors but $\mathbb{Z}$ does not.

(1.5) Questions on units in $\mathbb{Z}$

(a) In (1.3(c)) you found the units of $\mathbb{Z}$. Show they divide each element of $\mathbb{Z}$.

(b) Let a and b be non-zero integers satisfying $a|b$ and $b|a$. Show there exists a unit u such that $a = ub$.

(c) Show that $\mathbb{Z}/4\mathbb{Z}$ contains 2 non-zero elements whose product is zero.

To show (1.5(b)) you need the fact that if x is a non-zero integer and if $yx = 0$, then $y = 0$; in other words, that in $\mathbb{Z}$, the product of two non-zero elements is always non-zero. This is another way of saying that $\mathbb{Z}$ has no zero-divisors.

Answers to (1.5)

(a) $a = 1 \times a = (-1) \times (-a)$ for all $a \in \mathbb{Z}$

(b) If $b|a$, then $a = ub$ for some $u \in \mathbb{Z}$. If $a|b$ then $b = va$ for some $v \in \mathbb{Z}$. Hence $a = uva$ and so

$$(1 - uv) \times a = 0.$$

Since a is supposed to be *non-zero*, it follows that $(1 - uv) = 0$. Hence $uv = 1$ and u is a unit.

(c) Now $2 \not\equiv 0$ but $2 \times 2 \equiv 0 \bmod 4$.

The absence of zero divisors allows cancellation

Suppose that $a \neq 0$ and

$$ax = ay \tag{1.b}$$

in a system without zero divisors. Then $a\,(x - y) = 0$ and so $x - y = 0$, in other words $x = y$. Thus the non-zero a in Equation 1.b can be **cancelled**.

We can discuss divisors and units in algebraic systems other than $\mathbb{Z}$. Make the minimal assumption that the system is closed under multiplication.

(1.6) Questions on units in other systems

(a) The set $2\mathbb{Z}$ of **even** integers is closed under multiplication. Does the concept of unit make sense in $2\mathbb{Z}$?

(b) What are the units in $\mathbb{N}$?

(c) What are the units in $\mathbb{Q}$, the set of rational numbers?

Answers to (1.6)

(a) It does not make sense, because $2\mathbb{Z}$ does not have a 1 (sometimes called an **identity** or a **neutral element** with respect to multiplication).

(b) 1 is the only unit in $\mathbb{N}$.

(c) Every *non-zero* element is a unit in $\mathbb{Q}$.

You should convince yourself that $\mathbb{Z}[i]$ is closed under multiplication and contains 1.

Hint: Use the fact that if $uv = 1$ then

$$|u|^2|v|^2 = |uv|^2 = 1^2 = 1$$

and work out the modulus of

$$m + in.$$

(1.7) Further questions on units in other systems

(a) Now work in the system $\mathbb{Z}[i]$ of **Gaussian integers**, which are complex numbers of the form $m+in$ where m and n are integers. Thus in symbols

$$\mathbb{Z}[i] = \{m + in \in \mathbb{C} \mid m, n \in \mathbb{Z}\}.$$

Find the units of $\mathbb{Z}[i]$ (there are exactly four of them).

(b) Prove that a unit in an algebraic system divides every element of that system.

(c) Prove that a unit can not be a zero-divisor.

Answers to (1.7)

(a) Let u be a unit in $\mathbb{Z}[i]$. Then $\exists v \in \mathbb{Z}[i]$ such that $uv = 1$, and so $|u||v| = |uv| = |1| = 1$. By definition of Gaussian integers, there exist integers a, b, c and d such that $u = a + ib$ and $v = c + id$. Hence $(a^2 + b^2)(c^2 + d^2) = |u|^2|v|^2 = (|u||v|)^2 = 1^2 = 1$ and so $a^2 + b^2$ is a unit in $\mathbb{Z}$. Hence $a^2 + b^2 = 1$ (it cannot be -1, being positive!) and the only solutions in integers are $a = \pm 1, b = 0$ and $a = 0, b = \pm 1$. These in turn give four possibilities: $u = \pm 1$ or $\pm i$.

(b) If $uv = 1$, then $a = 1.a = (uv)a = u(va)$, whence u divides a.

(c) Let $uv = 1$. Then $au = 0$ implies that $a = a1 = auv = 0v = 0$. So u is not a zero-divisor.

2 Division with Remainder

Now we revise some ideas and results from *Foundations*. Much of Number Theory grows out of questions about the natural numbers. (Can we solve $a^3+b^3=c^3$ with $a,b,c\in\mathbb{N}$? Is every even integer greater than 4 the sum of 2 odd prime numbers?) Such questions soon lead into a larger arena: to be able to subtract, move the action to $\mathbb{Z}$, and to divide go to $\mathbb{Q}$, to use methods from *Analysis* extend your realm to $\mathbb{R}$, and to solve equations take $\mathbb{C}$ as your universe.

(2.1) Sort the following numbers into the sets $\mathbb{N}$, $\mathbb{Z}\backslash\mathbb{N}$, $\mathbb{Q}\backslash\mathbb{Z}$, $\mathbb{R}\backslash\mathbb{Q}$, $\mathbb{C}\backslash\mathbb{R}$:

$$\frac{-4}{4},\ 0,\ \frac{\sqrt{8}}{\sqrt{2}},\ \frac{-\sqrt{2}}{\sqrt{8}},\ \frac{\sqrt{3}}{\sqrt{8}},\ 1.4141\dot{5}\dot{9}\dot{9},\ \pi,\ e^{i\pi},$$

the roots of x^2-8, the roots of x^2+x+1.

Notice the different kinds of ambiguity in the notation we use to describe numbers. Each rational number can be described in infinitely many ways as a rational and in two ways as a decimal.

Answers to (2.1)

- $\mathbb{N}$ contains $\sqrt{8}/\sqrt{2}=2$.
- $\mathbb{Z}\backslash\mathbb{N}$ contains $-4/4(=-1), 0$ and $e^{i\pi}(=-1)$.
- $\mathbb{Q}\backslash\mathbb{Z}$ contains $-\sqrt{2}/\sqrt{8} = -1/2$ and $1.4141\dot{5}\dot{9}\dot{9} = 141416/1000000$.
- $\mathbb{R}\backslash\mathbb{Q}$ contains $\sqrt{3}/\sqrt{8}, \pi$ and the two roots of x^2-8.
- $\mathbb{C}\backslash\mathbb{R}$ contains the two roots $(-1\pm i\sqrt{3})/2$ of x^2+x+1.

(2.2) Write down the sequence obtained by subtracting 17 from 105 until the answer is negative.

Answer to (2.2) $105, 88, 71, 54, 37, 20, 3, -14$.

(2.3) How many subtractions did you use to reach the last non-negative term in the sequence ?

Answer to (2.3) 6

(2.4) Work out $\frac{105}{17}$ to four decimal places.

Answer to (2.4) 6.1765

(2.5) Write $\frac{105}{17}$ in the form $n + x$ with $n \in \mathbb{Z}$ and $0 \leq x < 1$ and then work out $17n$ and $17x$.

Answer to (2.5) $n = 6$ and $x = \frac{105}{17} - 6 = \frac{3}{17}$.

$$\begin{aligned} 17n &= 17 \times 6 = 102 \\ 17x &= 17 \times \frac{3}{17} = 3. \end{aligned}$$

(If you wrote $x = 0.1765$, which is only approximate, you would only have obtained the approximate value $17x = 3.0005$, but in fact $17x$ is an integer,)

(2.6) Find the integers q and r such that $105 = 17q + r$ with $0 \leq r < 17$.

Answer to (2.6) $q = 6$ and $r = 3$.

Notice that repeated subtraction is equivalent to division with remainder.

(2.7) Find $n \in \mathbb{Z}$ and $x \in \mathbb{R}$ such that $\frac{1066}{69} = n + x$ with $0 \leq x < 1$.

Answer to (2.7) $n = 15$ and $x = \frac{31}{69} \approx 0.4492754\cdots$

(2.8) Compute $1066 - 69n$ and $69x$. Compare the answers.

Answer to (2.8) $1066 - 69 \times 15 = 31$ and $69x = 31$.

Notice from the previous examples that $q = [a/b]$ and $r = a - qb$. To find q on your calculator, work out a/b and ignore everything to the right of the decimal point.

(2.9) Use your calculator to find q and $r \in \mathbb{Z}$ such that (i) $a = qb + r$ and (ii) $0 \leq r < b$ when (a, b) is in turn equal to:

$$\begin{array}{ccc} (100, 1) & (-21, 2) & (1001, 101) \\ (-1001, 101) & (1111, 101) & (2010, \text{your age}). \end{array}$$

Answer to (2.9)

$$\begin{aligned} 100 &= 100 \times 1 + 0 \\ -21 &= (-11) \times 2 + 1 \\ 1001 &= 9 \times 101 + 92 \\ -1001 &= (-10) \times 101 + 9 \\ 1111 &= 11 \times 101 + 0 \\ 2010 &= 111 \times 18 + 12 \\ &= 105 \times 19 + 15 \\ &= 100 \times 20 + 10 \ldots \end{aligned}$$

depending on your age!

(2.10) Definition If $x \in \mathbb{R}$, the notation $[x]$ means the greatest integer less than or equal to x. It is called the **integral part** (or the **round-down** or the **floor** of x). (An alternative notation is $\lfloor x \rfloor$.) Thus $[\pi]$ and $[3]$ are both equal to 3.

(2.11) Theorem Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Set $q = \left[\frac{a}{b}\right]$ and $r = \left(\frac{a}{b} - q\right) \times b$. Then

$$a = qb + r$$

with $0 \leq r < b$ and $r \in \mathbb{N}$.

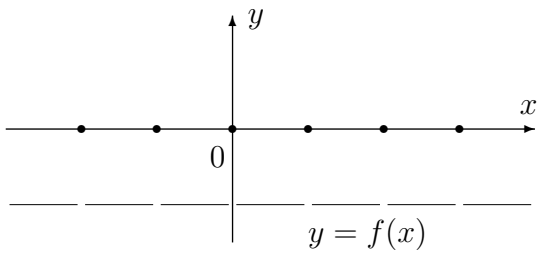
(2.12) Work out $[-5.2]$, $[\pi]$, $[-\pi]$, $\left[\frac{2010}{69}\right]$, $[\sqrt{2010}]$, $[x]$, when x is the larger root of $x^2 + 9x - 4$.

Answer to (2.12) $-5.2 = -6 + 0.8$ so $[-5.2] = -6$, $[\pi] = 3$, $[-\pi] = -4$, $\left[\frac{2010}{69}\right] = 29$, $[\sqrt{2010}] = 44$ and $[x] = 0$ (since $x = (-9 + \sqrt{97})/2$ and $9 < \sqrt{97} < 10$).

(2.13) Describe the graph of the function $f(x) = [x] + [-x]$.

Answer to (2.13)

$$f(x) = \begin{cases} 0 & \text{if } x \in \mathbb{Z} \\ -1 & \text{otherwise} \end{cases}$$



(2.14) Write down all the primes up to $\sqrt{2011}$,

$$p_1 < p_2 < \cdots < p_s < \sqrt{2011}.$$

Calculate the successive remainders when 2011 is divided by

$$p_1, p_2, \ldots, p_s.$$

What can you conclude about 2011?

Answer to (2.14)

p_i	2	3	5	7	11	13	17
Remainder	1	1	1	2	9	9	5
p_i	19	23	29	31	37	41	43
Remainder	16	10	10	27	13	2	33

2011 is a prime.

(2.15) Work out the remainders $r(20)$, $r(4)$, $r(5)$ when 2011 is divided by 20, 4 and 5 respectively. Compare $r(4)$ (resp. $r(5)$) with the remainder when $r(20)$ is divided by 4 (resp. 5)

Answer to (2.15)

$$\begin{aligned} 2011 &= 100 \times 20 + 11 \\ &= 502 \times 4 + 3 \\ &= 402 \times 5 + 1 \end{aligned}$$

$$\begin{aligned} r(20) = 11 &= 2 \times 4 + 3 \ (r(4) = 3) \\ &= 2 \times 5 + 1 \ (r(5) = 1) \end{aligned}$$

Questions and Conclusions from Section 2

- To find q and r such that $a = qb + r$ with $0 \leq r < b$, use your calculator to work out $q = [a/b]$, the integral part of a/b, and then compute $a - qb$ to get r.
- 2.14 suggests that if $p_1, \ldots, p_r$ are the primes up to $\sqrt{n}$, and if each p_i does not divide n, then n is a prime. Prove this fact.
- Suppose that c divides b, then let $r(b)$ (resp, $r(c)$) be the remainder on dividing a by b (resp, by c). 2.15 suggests that $r(c)$ is the remainder on dividing $r(b)$ by c. Give a proof of this fact.