5. INTEGERS AND DIVISIBILITY

§5.1. Divisibility

We discussed the definition and simple properties of the system of **integers** in Chapter 1. Within this system we have the system of **natural numbers** (often called the **counting numbers** or the **non-negative integers**). A fundamental property of the natural numbers is that every non-empty set of natural numbers has a least. This can be proved by the axiom of induction.

Theorem 1: Every non-empty set of natural numbers has a least.

Proof: Let $[n] = \{k \mid 0 \leq k \leq n\}$.

We prove by induction on n that every non-empty subset of [n] has a least.

If $n = 0$, the only non-empty subset of [0] is {0} itself and clearly 0 is its least element. So the statement is true for $n = 0$.

Suppose it is true for n and let S be a non-empty subset of [n + 1].

Case 1: n + 1 $\notin$ S: Then S $\subseteq$ [n] and so, by induction, has a least.

Case 2: n + 1 $\in$ S: Let T = S – {n + 1}.

Case 2A: T = ∅: Then S = {n + 1} which clearly has a least, namely n + 1.
Case 2B: T ≠ ∅: Then T ⊆ [n] and so has a least and clearly this is the least element of S.
Hence the statement is true for n + 1 and so, by induction, it is true for all n.

Now this only shows that every finite non-empty set of natural numbers has a least.
Suppose that S is any non-empty subset of ℕ. Let $n \in$ S.
Then S ∩ [n] ⊆ [n] and is non-empty.
So S ∩ [n] has a least, say m.
If $k \in$ S then and $k \geq n$ then $m \leq n \leq k$ and so $m \leq k$.
If $k < n$ then $k \in$ S ∩ [n] and so $m \leq k$.
So m is the least element of S. ✋☺

Theorem 2 (Division Algorithm): If m, n are integers, where m ≠ 0, then $n = m$q + r for some r with $0 \leq r < |m|$.
Proof: Let r be the least element of the set S = {$n - mq$ | $q \in \mathbb{Z}$} ∩ ℕ.
Suppose $r = n - mq \geq |m|$.

If $m > 0$ then this means that $r \geq m$. But $0 \leq r - m = n - m(q + 1) \in$ S, contradicting the fact that r is the least element of S.

If $m < 0$ then $|m| = -m$ and so $r \geq -m$. But $0 \leq r + m = n - m(q - 1) \in S$, again contradicting the fact that r is the least element of S.

Hence $0 \leq r < |m|$. ✋☺

We call r the **remainder** on dividing n by m. If the remainder is zero, that is if $m = nq$ for some $q \in \mathbb{Z}$, we say that m **divides** n. We write this as $\boldsymbol{m \mid n}$.
Equivalently we can say that n is a **multiple** of m.

Example 2: 3 divides 12, −17 divides 34, both 1 and −1 divide every number. Despite the maxim "you can't divide by 0" it *is* true that 0 divides 0, because $0 = 0q$ for all integers q. So $0 \mid 0$, even though $0 \div 0$ is undefined.
Make sure you don't confuse $m \mid n$ with m/n or $m \div n$. The expression $m \mid n$ is a statement. It can only be true or false. But m/n (equivalently $m \div n$) is a number.

We denote the set of divisors of n by $\mathbf{D(}\boldsymbol{n}\mathbf{)}$ and the set of multiples of n by $n\,\mathbb{Z}$.

Example 3:
$D(12) = \{\pm1, \pm2, \pm3, \pm4, \pm6, \pm12\}$, $12\,\mathbb{Z} = \{0, \pm12, \pm24, \pm36, \ldots\}$.
$D(1) = \{\pm1\}$, $1\,\mathbb{Z} = \mathbb{Z}$.
$D(0) = \mathbb{Z}$ (because $n = n.0$ for all n).
$0Z = \{0\}$.
$D(n)$ is finite for all n, except where $n = 0$.

$n\,\mathbb{Z}$ is infinte for all n, except where $n = 0$.

The set of **common divisors** of m, n is simply $D(m) \cap D(n)$. Associated with this is $\boldsymbol{m}\mathbb{Z} + \boldsymbol{n}\mathbb{Z}$ which is the set of all numbers of the form $mh + nk$ where $h, k \in \mathbb{Z}$.

Theorem 3: For all integers m, n we have $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ for some $d \in \mathbb{Z}$.
Proof: Let d be the smallest positive element of $m\mathbb{Z} + n\mathbb{Z}$.
Then $d = mh + nk$ for some $h, k \in \mathbb{Z}$.
Clearly any multiple of d will belong to $m\mathbb{Z} + n\mathbb{Z}$ and so $d\mathbb{Z} \subseteq m\mathbb{Z} + n\mathbb{Z}$.

Now let $k = ma + nb \in m\,\mathbb{Z} + n\,\mathbb{Z}$. Let r be the remainder on dividing k by d.
That is, $k = ma + nb = dq + r$ for some $q \in \mathbb{Z}$ and $0 \leq r < d$.
Now $r = ma + nb - (mh + nk)q = m(a - hq) + n(b - kq) \in m\mathbb{Z} + n\,\mathbb{Z}$. But d is the smallest positive element of $m\mathbb{Z} + n\mathbb{Z}$, so it must be that $r = 0$. Hence $k = dq \in d\mathbb{Z}$ and so $m\mathbb{Z} + n\mathbb{Z} \subseteq d\mathbb{Z}$.
Hence $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$. ✋☺

Suppose m, n are non-zero integers. Then $D(m) \cap D(n)$ is finite. An element of this set of largest absolute value is called a **greatest common divisor** of m, n.

Example 4: D(15) = {±1, ±3, ±5, ± 15} and D(51) = {±1, ±3, ±17, ±51} so
D(m) ∩ D(n) = {±1, ±3}. The elements with largest absolute value are ±3, so these are both greatest common divisors of 15 and 51.

Theorem 4: If $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ then d is a greatest common divisor of m, n.
Proof: Let $d = mh + nk$. If e is a common divisor of m, n then $e \mid d$ and so d is a greatest common divisor. ✋☺
Corollary: A GCD of m, n can be expressed in the form $mh + nk$.

Clearly every pair of non-zero integers has exactly 2 greatest common divisors, $\pm d$. However, when we refer to ***the* greatest common divisor** we mean the positive one. We denote this by **GCD(m, n)**. By Theorem 4 GCD(m, n) = $mh + nk$ for some $h, k \in \mathbb{Z}$.

Example 5: GCD(91, 230) = 13, GCD(56, 27) = 1.

Two non-zero numbers m, n are defined to be **coprime** if GCD(m, n) = 1. Loosely speaking we might say that they have "no common factors", but what we'd really mean is that the only common factors are ±1.

If we divide two numbers by their GCD the quotients will become coprime because we'd have removed all the common factors.

Theorem 5: If d = GCD(a, b) then a/d and b/d are coprime.
Proof: Let $a = a_0 d$ and $b = b_0 d$ and let e = GCD(a_0, b_0).
Let $a_0 = a_1 e$ and $b_0 = b_1 e$.
Then $a = a_1 ed$ and $b = b_1 ed$ and so ed is a common divisor of a, b.
Since d is the greatest common divisor it must be that e = 1. ✋☺

§5.2. The Euclidean Algorithm

There most obvious way of finding the greatest common divisor of two numbers is to factorise each of them. This, however, is highly inefficient. Factorising numbers is extremely time consuming, even with the help of a computer, unless the numbers are small. But long before computer the ancient Greeks had devised a very efficient method of finding GCDs.

The Euclidean Algorithm:
To find the GCD of two positive numbers:
(1) Divide the smaller into the larger getting a quotient and remainder.
(2) Replace the larger number by this remainder.
(3) While the smaller number is positive go to step (1) and continue.
(4) When the smaller number becomes zero, the larger is the required GCD.

Example 6: Find GCD(1131, 2977).
Solution: $2977 = 1131.2 + 715$
$1131 = 715.1 + 416$
$715 = 416.1 + 299$
$416 = 299.1 + 117$
$299 = 117.2 + 65$
$117 = 65.1 + 52$
$65 = 52.1 + 13$
$52 = 13.4 + 0$
The last non-zero remainder is 13 and so GCD(1131, 2977).

By the Corollary to Theorem 4 we can write 13 in the form $1131h + 2977k$ for some numbers h, k.

Example 7: Find integers h, k such that $13 = 1131h + 2977k$.
Solution: We work back through the above calculations.
$13 = 65 – 52$

$= 65 – (117 – 65) = 65.2 – 117$
$= (299 – 117.2).2 – 117 = 299.2 – 117.5$
$= 299.2 – (416 – 299).5 = 299.7 – 416.5$
$= (715 – 416).7 – 416.5 = 715.7 – 416.12$
$= 715.7 – (1131 – 715).12 = 715.19 – 1131.12$
$= (2977 – 1131.2).19 – 1131.12 = 2977.19 – 1131.50$

So $h = –50$, $k = 19$ is one solution.

You must resist the temptation to simplify, except as a check. Keep the two current numbers intact at all times. However at the end you should check that the expression simplifies to the GCD.

Theorem 6: Euclid's algorithm finds the GCD of two positive integers.

Proof: Let m, n be positive integers. Suppose $m = nq + r$ where $0 \leq r < m$.

Then $D(m) \cap D(n) = D(n) \cap D(r)$ since any k that divides both m, n divides r and any k that divides both n, r divides m. Hence $GCD(m, n) = GCD(n, r)$. ✋☺

Theorem 7: If $m|ab$ and $GCD(a, m) = 1$ then $m|b$.

Proof: By Theorem 4, $1 = ah + mk$ for some $h, k \in \mathbb{Z}$ and so $b = abh + mkb$.

Since $m|ab$, $m|b$. ✋☺

§5.3. The One-Way Euclidean Algorithm

The reverse algorithm is unpleasant to perform and is error prone, yet it's important to a number of applications, such as finding inverses modulo *m*. This tabular version involves about half the arithmetic and a quarter of the writing as the usual method and proceeds in a single direction by computing the ingredients for the inverse as we go instead of having to work backwards.

To find the GCD of *a*, *b* and to express it in the form *ah* + *bk* proceed as follows:

A	**Q**	**B**
a		0
b		1
…	…	…
A′	…….	B′
A	*q* = INT(A′/A)	B
A′ – A*q*		B′ – *q*B
…	…	…
GCD		**k**
0	← STOP	

The pattern for each of the outside columns is "up two minus down times across"

The first column contains the successive remainders and the last non-zero remainder will be the GCD. In the third column, opposite the GCD will be a suitable value of k. Having found k the corresponding value of h is simply $h = \frac{\text{GCD} - bk}{a}$.

Examples 6 and 7 revisited: Find GCD(2977,1131) and express it in the form $2977h + 1131k$.

A	**Q**	**B**
2977		0
1131	2	1
715	1	–2
416	1	3
299	1	–5
117	2	8
65	1	–21
52	1	29
13	4	**–50**
0		

Hence GCD(2977,1131) = 13 and $k = -50$ and $h = \frac{13 - 1131(-50)}{2977} = \frac{56563}{2977} = 19$.

Hence $13 = 2977.19 - 1131.50$.

Example 8: Find the inverse of 30 modulo 143.

A	Q	B
143		0
30	4	1
23	1	–4
7	3	5
2	3	–19
1		62

Hence $30^{-1} \equiv 62 (\text{mod } 143)$.

§5.4. Prime Numbers

A **unit** in any algebraic system is an element that has an inverse within that system. The units of the system of real numbers are all the non-zero elements, but in $\mathbb{Z}$. the only units are ± 1

We define a number p to be **prime** if it is non-zero, not a unit and the only divisors of p are units and p times a unit. In $\mathbb{Z}$ this means that the only divisor of a prime p are ± 1 and $\pm p$. Note that we rule out ± 1 from being prime.

Why don't we allow 1 or –1 to be called prime? There is no logical reason why they couldn't be included. It is just a matter of convenience. The units ± 1 have special

properties and if we included them as primes we'd often have to often say "prime number except ± 1" in our theorems.

Example 9: The prime numbers are ±2, ±3, ±5, ±7, ±11, ±13, ±17, ±19, ±23, ±31, …

Numbers that are not prime, other than the three special numbers −1, 0, and 1, are called **composite**. There are four basic sets of numbers according to this classification.

0	**±1**	**prime numbers**	**composite numbers**

Theorem 9: If p is prime and $p \mid ab$ then $p|a$ or $p|b$.
Proof: Suppose that p is prime and suppose that p dies not divide a. Then GCD(a, p) = 1 and so, by Theorem 7, p|b.

It's a very useful fact that every number can be factorised into primes. Well, that's not strictly true. Zero can't be factorised into primes. What about ±1? We can include them if we allow a product of zero primes to be defined Let's keep to numbers whose absolute value is bigger than 1. Is it true that "every number whose absolute value is bigger than 1 can be factorised uniquely into primes"? That depends on what we would consider to be a different factorisation.

Example 10: There are 4 factorisations of 6 into primes: $6 = 2.3 = 3.2 = (-2)(-3)$. We consider all four factorisations to be the one factorisation.
Note that if we allowed 1 and –1 to be primes we would have infinitely many prime factorisations of 6. For example $6 = (-2).3.(-1).1.1.1.(-1)(-1)$.

Theorem 10: (Fundamental Theorem of Arithmetic)
If $|n| > 1$ then $n = p_1p_2 \dots p_h$ for some h and some primes $p_1, p_2, \dots, p_h$.
Moreover if $n = p_1p_2 \dots p_h = q_1q_2 \dots q_k$ then $h = k$ and after suitable rearrangement of the factors
$p_i = \pm q_i$ for each i.
Proof: We prove the first part by induction on $|n|$. Suppose that numbers whose absolute value is smaller than $|n|$ can be factorised into primes.
If n is prime then $h = 1$ and $p_1 = n$.
If n is composite then $n = ab$ for some numbers a, b where $|a|$ and $|b|$ are bigger than 1.
Since $|a|$ and $|b|$ are smaller than $|n|$ it follows by the strong principle of induction that each of a, b can be factorised into primes and hence so can n.

We prove the second part by induction on the number of prime factors, h. Suppose that
$p_1p_2 \dots p_h = q_1q_2 \dots q_k$. Then p_1 divides $q_1q_2 \dots q_k$ and so p_1 divides q_j for some j, by Theorem 4. Since q_j is prime and $p_1 \neq \pm 1$, this means that $p_1 = \pm q_j$. Rearranging the factors and dividing by p_1 we get $p_2 \dots p_h = (\pm q_1)q_2 \dots q_k$.

By induction $h - 1 = k - 1$ and for each $i \geq 2$, $p_i = \pm q_j$ for some
$j \geq 2$. ✋☺

§5.5. Generating Prime Numbers

There is no known formula for the n'th prime number. At least there are formulae but they that are so impractical to use they are worse than no formula at all. There is virtually no improvement on the simple-minded approach of testing all possible factors.

One obvious improvement is the fact that we only need to test for factors up to $\sqrt{n}$.

Theorem 11: If p has no factors n for $2 \leq n \leq \sqrt{p}$ then p is prime.
Proof: If $p = ab$ where $1 < a, b < p$ then one of a, b must be less than or equal to $\sqrt{p}$ (If they were both bigger than $\sqrt{p}$ then ab would be bigger than p. ✋☺

Another improvement is that if we are generating all primes, by the time we got to p we would have a list of all primes less than p. So we never need to test for divisibility by numbers that are composite. If we are just testing a single number p, and don't have a list of primes less than p then at least we should not be testing divisibility by numbers that are clearly composite, such as even numbers and multiples of 3 or 5.

It is useful to be able to recognise multiples of 2, 3 and 5.

Multiples of 2are those numbers that end in 0, 2, 4, 6 or 8.
Multiples of 5 are those numbers that end in 0 or 5.
Multiples of 3 are those numbers where the sum of the digits is a multiple of 3.

Example 11: Is 3197 prime?
Solution: $\sqrt{3197} = 56.542\ldots$ so we only need to test by numbers up to 56. But 56, 55 and 54 are clearly composite so in fact we need only go up to 53.
3197 is clearly not divisible by 2, 3 or 5. So, using our calculator we test for 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53.
We discover that 23 is a factor and that 3197 = 23.139.

Example 12: Is 5113 prime?
Solution: $\sqrt{5113} = 71.50\ldots$ so we only need to test by numbers up to 71.
5113 is clearly not divisible by 2, 3 or 5. So, using our calculator we test for 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71. Since 5113 is not divisible by any of these it must be prime.

An ancient method for generating primes is known as the sieve of Eratosthenes. It is particularly suitable if you happen to live in an ancient civilization without calculators. You write down a list of all numbers, in order from 2 to some large number. You circle the '2' and then cross out every 2^{nd} number after that.

At each stage you circle the first number that has not been crossed out. That will be a prime number. If this is p then you cross out every p^{th} number after that. Continue until every number has been circled or crossed out. The circled numbers will be prime and the crossed out ones will be composite.

Example 13: Use the sieve of Eratosthenes to find all the primes up to 100.

Solution:

	(2)	(3)	~~4~~	(5)	~~6~~	(7)	~~8~~	~~9~~	~~10~~
(11)	~~12~~	(13)	~~14~~	~~15~~	~~16~~	(17)	~~18~~	(19)	~~20~~
~~21~~	~~22~~	(23)	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	(29)	~~30~~
(31)	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	(37)	~~38~~	~~39~~	~~40~~
(41)	~~42~~	(43)	~~44~~	~~45~~	~~46~~	(47)	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	(53)	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	(59)	~~60~~
(61)	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	(67)	~~68~~	~~69~~	~~70~~
(71)	~~72~~	(73)	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	(79)	~~80~~
~~81~~	~~82~~	(83)	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	(89)	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	(97)	~~98~~	~~99~~	~~100~~

Notice that as numbers get larger, primes become rarer. In successive groups of 10 the percentage of primes is 40%, 40%, 20%, 20%, 30%, 20%, 20%, 30%, 20%, 10%, giving 25% over the first 100. The percentage of primes up to 1000 drops to 16.8%. In the first 10,000 it is only about 12% and in the first million it is less than 8%. Could it be that primes become so rare that they finish altogether? Is there in fact a largest prime?

Of course there are infinitely many numbers altogether, but even if there were only finitely many primes there would still be infinitely many numbers. After all there are infinitely many powers of 2 and that uses just one prime. This question was asked, answered, a long time ago by the ancient Greeks.

Theorem 12: (EUCLID) There are infinitely many primes.
Proof: The simple method of showing that there are infinitely many numbers is to say, "if there is a biggest number just add 1 and you get a bigger one". This doesn't work for primes because adding 1, or even 2 to a prime does not always give a prime. But we can do something a little bit similar.

Suppose there is a largest prime N. Now take N! = N(N – 1)(N – 2) … 3.2.1. Every prime divides N! because every prime will appear as one of its factors. Now take N! + 1. No prime number will divide it because they all divide N! and no number bigger than 1 can divide two successive numbers. But every number bigger than 1 is divisible by a prime number, so we get a contradiction. Hence there are infinitely many prime numbers. ✋☺

EXERCISES FOR CHAPTER 5

Exercise 1: Factorise 2926 into prime factors.

Exercise 2: Factorise 713 into primes.

Exercise 3: Show that 659 is prime.

Exercise 4: Find the first prime after 1000.

Exercise 5: Find the GCD of 11111 and 3403.

Exercise 6: Find the GCD of 10101 and 5019.

SOLUTIONS FOR CHAPTER 5

Exercise 1: 2926 = 2.1463.
We now try dividing 1463 by 3, 5, 7, 11, …and discover that it is exactly divisible by 7.
So 2926 = 2.7.209 = 2.7.11.19.

Exercise 2: We try dividing by the primes 3, 5, 7, 11, …and eventually discover that
713 = 23.31.

Exercise 3: $\sqrt{659} = 25.6\ldots$ so we only need to check for divisibility by primes up to 23.

Since none of these primes divide 659 we can conclude that 659 is prime.

Exercise 4: $\sqrt{1000} = 31.6$ so we will only need to check for prime divisors up to 31 (unless it turned out that there are no primes between 1000 and $33^2 = 1089$).
1001 = 7.143
1003 = 17.59
1007 = 19.53
1009 is prime.

Exercise 5:

3	3	1	3	2
3403)11111	902)3403	697)902	205)697	82)205
10209	2706	697	615	164
902	697	205	82	41

Since 41 divides 82 the next remainder will be zero, so the last non-zero remainder is 41. Hence the GCD of 11111 and 3403 is 41.

Exercise 6: $10101 = 5019 \times 2 + 63$
$5019 = 63 \times 79 + 42$
$79 = 42 + 37$
$42 = 37 + 5$
$37 = 5 \times 7 + 2$
$5 = 2 \times 2 + 1$
So GCD(10101, 5019) = 1.