Number and Arithmetic

God created the natural numbers, and all the rest is the work of man. *Leopold Kronecker*

Number Systems

You have, of course, been using numbers for most of your life. Why then do we need to talk about number systems here?

1. They make a good starting point to introduce rigour to your thought processes.
2. Because we need to understand the relationship between computer arithmetic and mathematical arithmetic, and that can only be done with a sound understanding of the latter.
3. Thirdly, we will need to define some variants of standard arithmetic, and need a firm foundation before we do that.

It is important to remember that we are studying the abstract (or pure) number systems, not their implementation on computers.

Natural Numbers

The natural numbers, denoted by $\mathbb{N}$, is defined to be the set of counting numbers including zero:

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}. \tag{1}$$

Zero is included for (good) technical mathematical reasons that don't concern us here.

For every natural number n we can define its successor Sn as $Sn = n + 1$. A key property of the natural numbers is that every natural number can be reached from zero by applying the successor function S a finite number of times.

Successor and Loop

The successor function maps directly onto the idea of a loop in programming languages.

```
1    -- Output a line of stars
2    FOR Index IN Margin + 1 .. Margin + Length LOOP
3       Put("*");
4    END LOOP;
```

- The `Integer` variables `Margin` and `Length` are assumed to be initialised before the start of the loop. The index variable `Index` counts through the `Length` repetitions of the loop.
- If `Length` is less than or equal to zero, then the body of the loop is not executed at all (i.e. is executed zero times). This partly explains why the natural numbers include zero.

Induction

We can prove statements about natural numbers by a technique called induction. Suppose that we can prove the following two statements about a property $P(n)$:

1. $P(0)$ is true;
2. if $P(n)$ is true then $P(n+1)$ is true.

Then $P(n)$ is true for all natural numbers n.

This is a very useful tool, as it means that we only need to prove one special case (which is usually very easy) and one general case which involves a small step (from n to $n+1$). Induction is often used when proving the correctness of an algorithm, particularly if it involves a loop. Here $P(n)$ is the statement that the algorithm is correct for an input value of n.

Arithmetic Operations

- It is clear that if you add or multiply two natural numbers, you get another natural number. The technical phrase for this is that "$\mathbb{N}$ is closed under addition and multiplication".
- $\mathbb{N}$ is not closed under subtraction or division: give one counterexample of each (i.e. one pair of numbers for which subtraction takes you outside $\mathbb{N}$, and one pair of numbers for which division takes you outside $\mathbb{N}$).

Solution

$\mathbb{N}$ is not closed under subtraction or division: give one counterexample of each (i.e. one pair of numbers for which subtraction takes you outside $\mathbb{N}$, and one pair of numbers for which division takes you outside $\mathbb{N}$).

$$1 - 2 \notin \mathbb{N}.$$

$$1/2 \notin \mathbb{N}.$$

This algebraic flaw is fixed in other number systems.

Radix Notation

- When we write down numbers we usually use decimal notation. Another way of putting this is that we are using a radix 10 representation.
- The Σ notation is a very compact way of expressing sums, i.e. adding up a collection of terms.
- If $a_1, \ldots, a_n$ are numbers, then $\sum_{i=1}^{n} a_i$ stands for $a_1 + \cdots + a_n$. Usually, a_i will be expressed as some algebraic formula. For example

$$\sum_{i=1}^{3} 2i + 1 = 3 + 5 + 7 = 15. \tag{2}$$

- Calculate

$$\sum_{i=0}^{3} 3i + 2.$$

Solution

Calculate

$$\sum_{i=0}^{3} 3i + 2.$$

$$\begin{aligned}\sum_{i=0}^{3} 3i + 2 &= (3 \times 0 + 2) + (3 \times 1 + 2) + (3 \times 2 + 2) + (3 \times 3 + 2) \\ &= 2 + 5 + 8 + 11 \\ &= 25.\end{aligned}$$

Representing Numbers

The usual representation of a natural number n has the form $a_k a_{k-1} \ldots a_2 a_1 a_0$ where each a_i is a digit: that is a natural number between 0 and 9. This means that

$$n = \sum_{i=0}^{k} a_i 10^i \tag{3}$$

where 10^i is 10 multiplied by itself i times. Remember that $10^1 = 10$ and $10^0 = 1$. For example, the two digits '4' followed by '2' represent the number

$$2 \times 10^0 + 4 \times 10^1 = 2 + 4 \times 10 = 2 + 40 = 42.$$

Write 5829 as a sum.

Solution

Write 5829 as a sum.

$$5829 = 5 \times 10^3 + 8 \times 10^2 + 2 \times 10^1 + 9 \times 10^0$$

Here, the number 10 is the radix of the representation. Any natural number $r > 1$ can be used. $r = 2$ gives the binary number system, familiar to all computer scientists.

Integers

- We have already commented that the natural numbers are not closed under subtraction. The set of integers (or whole numbers) $\mathbb{Z}$ solves that problem.

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \tag{4}$$

- Why $\mathbb{Z}$? The reason is that these number systems were formalised in the 19th century by German mathematicians, and 'Zahlen' is the German for numbers.
- We can now perform addition, multiplication and subtraction and stay safely inside the number system, but it is still possible to divide two numbers and move outside it (e.g. divide 1 by 2).
- We have lost the induction property. The successor function still exists (which is why Ada loops work with integer variables), but there is no longer a 'first element'. If you try to name one, I can always name another element that is smaller.

Prime Numbers

- Certain numbers form multiplicative building blocks for all the others. These are the primes: an integer greater than 1 is prime if the only numbers that divide it exactly are itself and 1. The first few primes are

$$2, 3, 5, 7, 11, 13, \ldots$$

- Every integer can be written uniquely as a product of primes.

$$n = p_1^{m_1} \cdots p_r^{m_r}. \tag{5}$$

  In this equation both the prime numbers p_i and the powers m_i are uniquely defined, provided that we exclude any $m_i = 0$, since these just give a value of 1.

- For example

$$18 = 2^1 \times 3^2 \qquad 42 = 2^1 \times 3^1 \times 7^1.$$

Prime Factorisation

- While we are guaranteed that every integer can be written as the product of primes, finding the prime factorisation of a large integer takes a long time. This has important consequences later when we come to look at coding algorithms.
- Testing whether a number is prime is a bit easier. In the simplest approach, we note that if n is not prime, then there must be a smaller number that divides it exactly. Also, if $n = lm$, then at least one of l and m can be no greater than $\sqrt{n}$, the square root of n. Thus an effective (if not super-efficient algorithm) is the following:

```
1   for l = 1..sqrt(n)
2     if l div n
3       return true;
4   end
5   return false;
```

- Use the algorithm to test whether 61 is prime.

Highest Common Factor

- It is often useful to be able to calculate the highest common factor of two numbers a and b (otherwise known as the greatest common divisor).
- We shall write $h = \text{hcf}(a, b)$ for this number. It is the largest integer that divides exactly into both a and b. For example, $\text{hcf}(24, 30) = 6$.
- What is the hcf of 18 and 25?

Algorithm for Computing H.C.F.

- We shall use the prime factorisations of a and b. Let $p_1, \ldots, p_n$ be the set of primes that divide either a or b, and write:

$$a = p_1^{l_1} \cdots p_n^{l_n} \qquad \text{and} \qquad b = p_1^{m_1} \cdots p_n^{m_n}.$$

  Here some of the powers l_i, m_i may be zero, unlike in (5).

- Then it is not hard to show that

$$\text{hcf}(a, b) = p_1^{k_1} \cdots p_n^{k_n}, \tag{6}$$

  where $k_i = \min(l_i, m_i)$. For example,

$$24 = 2^3 \times 3^1 \times 5^0 \qquad \text{and} \qquad 30 = 2^1 \times 3^1 \times 5^1. \tag{7}$$

  So $k_1 = 1$, $k_2 = 1$, and $k_3 = 0$. Hence
  $\text{hcf}(24, 30) = 2^1 \times 3^1 \times 5^0 = 6$, as before.

- Write down the prime factorisations of 18 and 25. Use them to calculate $\text{hcf}(18, 25)$.

Solution

Write down the prime factorisations of 18 and 25. Use them to calculate hcf$(18, 25)$.

$$18 = 2^1 \times 3^2 \times 5^0$$

$$25 = 2^0 \times 3^0 \times 5^2$$

Hence $l_1 = 1$, $l_2 = 2$, $l_3 = 0$; $m_1 = 0$, $m_2 = 0$, $m_3 = 2$. Thus $k_1 = k_2 = k_3 = 0$ and

$$\text{hcf}(18, 25) = 2^0 \times 3^0 \times 5^0 = 1 \times 1 \times 1 = 1.$$

Euclid's Algorithm

So we have a workable algorithm, but it is very inefficient because it depends on the prime factorisation. One of the most famous (and earliest) algorithms for any task is Euclid's algorithm for computing the hcf(a, b). It is based on the following argument.

- If $a \leq b$, then we can divide b by a to obtain a quotient q and a remainder r, where $0 \leq r < a$. This means that $b = qa + r$.
- Now, if $r = 0$, then a divides b, and hence hcf$(a, b) = a$ and we are done.
- Otherwise, it is easy to show that hcf$(a, b) =$ hcf(r, a). We can then continue by dividing r into a.
- Because $r < a$, we can guarantee that the algorithm will eventually terminate, and it is much more efficient than using the prime factorisation.

Euclid's Algorithm: Worked Example

Let us find the hcf of 568 and 208:

$$568 = 2 \times 208 + 152$$

$$208 = 1 \times 152 + 56$$

$$152 = 2 \times 56 + 40$$

$$56 = 1 \times 40 + 16$$

$$40 = 2 \times 16 + 8$$

$$16 = 2 \times 8 + 0$$

Thus $\text{hcf}(208, 568) = 8$.

Euclid's Algorithm II

- Euclid's algorithm provides extra information: it enables us to find integers m and n such that $ma + nb = \text{hcf}(a, b)$. (We shall see why this is useful when we look at cryptography).
- This is done by working backwards through the computation from the penultimate line.

$$
\begin{aligned}
8 &= 40 - 2 \times 16 \\
&= 40 - 2 \times (56 - 1 \times 40) = 3 \times 40 - 2 \times 56 \\
&= 3 \times (152 - 2 \times 56) - 2 \times 56 = 3 \times 152 - 8 \times 56 \\
&= 3 \times 152 - 8 \times (208 - 1 \times 152) = 11 \times 152 - 8 \times 208 \\
&= 11 \times (568 - 2 \times 208) - 8 \times 208 = 11 \times 568 - 30 \times 208
\end{aligned}
$$

- Use Euclid's algorithm to find $\text{hcf}(24, 30)$. Also find integers m and n such that $24m + 30n = \text{hcf}(24, 30)$.

Solution

Use Euclid's algorithm to find hcf$(24, 30)$. Also find integers m and n such that $24m + 30n = \text{hcf}(24, 30)$.

$$30 = 1 \times 24 + 6 \qquad\qquad 6 = 1 \times 30 - 1 \times 24$$

$$24 = 4 \times 6 + 0$$

Hence $6 = \text{hcf}(24, 30)$ and $6 = 1 \times 30 - 1 \times 24$.

Rational Numbers

- The next number system extends the integers so that it is closed under all four arithmetic operators: addition, subtraction, multiplication and division.
- This is the rational numbers $\mathbb{Q}$, which consists of integer fractions.
- Thus $\mathbb{Q}$ consists of all numbers that can be written in the form a/b with a and b in $\mathbb{Z}$ and $b \neq 0$.
- Why are the rational numbers important? Every decimal or binary number which recurs must be rational. Because a number that is represented on a computer only has a finite number of non-zero values after the decimal point, eventually it recurs (with the repeated value 0). Hence every number represented on a computer must be rational.

Rational Arithmetic

We can define the four arithmetic operators on $\mathbb{Q}$ as follows:

$$\frac{a_1}{b_1} +_{\mathbb{Q}} \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}$$

$$\frac{a_1}{b_1} -_{\mathbb{Q}} \frac{a_2}{b_2} = \frac{a_1 b_2 - a_2 b_1}{b_1 b_2}$$

$$\frac{a_1}{b_1} \times_{\mathbb{Q}} \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2}$$

$$\frac{a_1}{b_1} \div_{\mathbb{Q}} \frac{a_2}{b_2} = \frac{a_1 b_2}{b_1 a_2} \quad \text{if } a_2 \neq 0$$

We can easily show that $\mathbb{Q}$ extends $\mathbb{Z}$ by noting that the set of rationals of the form $a/1$ is equivalent to $\mathbb{Z}$.

Real Numbers

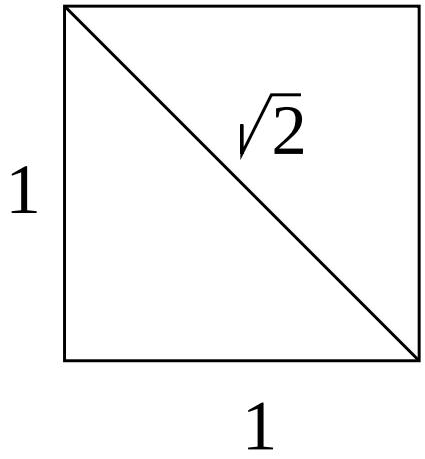
- The final number system we need is the real numbers, denoted by $\mathbb{R}$.
- We can take this system to be all the infinite decimal numbers (both recurring and non-recurring). To be precise, we must note that certain decimals are exactly the same. For example:

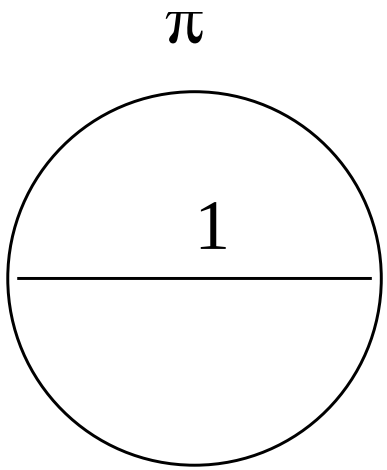
$$42.7899999\cdots = 42.79000000.$$

- Arithmetic on the real line is defined in the familiar way.

Real Numbers and Geometry

- Why do we need real numbers? The simple answer is that the rationals leave a lot of gaps.
- The real numbers represent all the points on a line: there are lengths that are not rational numbers, and these are called irrational numbers.
- Two famous examples of irrational numbers are $\sqrt{2}$ and π.





Summary

1. There are four main 'standard' number systems: natural numbers $\mathbb{N}$; integers $\mathbb{Z}$; rationals $\mathbb{Q}$; reals $\mathbb{R}$.
2. We must distinguish between mathematical definitions of number systems and their implementation in software.
3. Natural numbers are for counting; they are defined by a zero and a successor function $Sn = n + 1$.
4. The Σ notation is a compact way of expressing sums.
5. The integers add negative numbers to the natural numbers. There is no first element.
6. Prime numbers are the basic building blocks for the multiplicative structure of the integers. The prime factorisation of an integer is essentially unique.
7. Euclid's algorithm is an efficient method for computing the highest common factor of two integers.
8. Rational numbers are the ratio of two integers.
9. Real numbers are all infinite decimals.
10.
11.