Topics in Number Theory, Algebra, and Geometry

Ambar N. Sengupta

December, 2006

Contents

Introductory Remarks

These notes were written for a History of Mathematics class (Math 4700) at LSU in Spring 2006. There is, however, very little history in the notes. I chose a few topics, many of which are related to the Euclidean Algorithm, with roots in history, and followed their development, sometimes anachronistically.

In Chapter 1, we first begin with Euclid's algorithm (Book VII of his *Elements*) for finding the greatest common divisor of two numbers. The algorithm is then applied to deduce several basic results on divisibility, and eventually to two fundamental facts about numbers: every number greater than 1 is a product of primes in a unique way, and there are infinitely many primes. After this we return to Euclid's algorithm in the *geometric setting* (Book X of Euclid's *Elements*), of finding 'common measures of like magnitudes.' This leads to the notion of both rational numbers (those for which the Euclidean algorithm terminates) and irrational numbers (those for which the algorithm does not terminate), understood in terms of continued fractions, which emerge naturally from Euclid's geometric algorithm for the greatest common measure. We then develop the basic facts about continued fractions, and apply them to solving Pell's equation and simple Diophantine equations. We also take a look at the Fibonacci numbers in the context of continued fractions. The notes don't include additional material, such as the Chinese remainder theorem, and properties of the icosahedron, covered in class.

Chapter 2 examines topics in the theory of polynomials and polynomial equations. The role of the Euclidean algorithm, now in the setting of the algebra of polynomials, is underlined. The present form of the notes don't include all the topics in the theory of equations which were discussed in class, such as methods of solving cubic and quartic equations, and some facts about determinant and resultants.

Chapter 3 presents axiomatics, due to Hilbert, of Euclidean geometry, but the objective is to understand how the Euclidean axioms and geometric ruler-compass constructions (producing points and lines consistent with the axioms) lead to an algebraic structure:

- *ratios of segments can be added and multiplied, and these, together with* 0 *and negatives, form a field.*

With a sufficiently strong axiom of completeness, this is the field of real numbers.

Thus, from the Euclidean viewpoint, real numbers (or numbers in extensions of the field of rationals) are ratios of segments, or, more generally, of magnitudes. In class we also looked at projective geometry and, very briefly, conic sections. These are not discussed in the notes.

Historical dates cited are all taken from Wikipedia. References to Euclid's *Elements* are most conveniently looked up online at http://aleph0.clarku.edu/~djoyce/java/elements/elements.html

Hilbert's axioms are taken from Hilbert's book [1].

These notes have not been proof read carefully. I will update them time to time.

Chapter 1

Topics in Number Theory

We shall examine some key ideas of elementary number theory, from a historical, primarily Greek, viewpoint. Euclid, in his *Elements*, considers both *numbers* and *magnitudes*. Numbers are cardinal numbers, arising from counting, i.e. measuring sizes of abstract sets. Magnitudes are of geometric origin, measuring sizes of geometric sets, and include positive rationals and, if one is granted a powerful enough axiom system, all positive real numbers.

The central theme of this chapter will be Euclid's algorithm for finding the greatest common divisor of two numbers, and his corresponding algorithm for the common measure of two magnitudes.

1.1 Basic Notions and Notation

We need a few basic notions and notation first. These notions and notation arose in the 19th and 20th centuries, but will provide us with a convenient and precise language necessary to discuss mathematical concepts from antiquity.

A *set* is a collection of objects. These objects are called the *elements* of the set. We often display a set by listing its elements within brackets; for example,

$$S = \{a, b, c\}$$

displays a set S whose elements are a, b, and c. If x is an element of a set B then we denote this symbolically as:

$$x \in B.$$

Thus, in the example above, $a \in S$.

The set of *natural numbers* is

$$\mathbf{N} = \{1, 2, 3, ...\}.$$

The set of *integers* is

$$\mathbf{Z} = \{0, 1, -1, 2, -2, ...\}.$$

Sometimes we shall use the set of whole numbers:

$$\mathbf{W} = \{0, 1, 2, 3, ...\}.$$

The set which has no elements at all is called the *empty set* and is denoted

$$\emptyset.$$

To stress that a particular set is not empty, we will use the adjective 'non-empty.'

A fundamental fact about the natural numbers is the *principle of well-ordering*:

$$\textit{Every non-empty subset of } \mathbf{N} \textit{ has a least element.} \tag{1.1}$$

For example, the set of positive even numbers has 2 as its least element. This principle may seem at first to be too 'obvious' a fact to bother mentioning, but as we shall see, a vast body of facts about numbers can be established using this principle as a tool of reasoning. Such 'obvious' principles were not often recognized in the early days of mathematics.

An integer $x \in \mathbf{Z}$ is said to be a *factor* or *divisor* of an integer y if y is an exact multiple of x, i.e. if

$$y = mx,$$

for some integer $m \in \mathbf{Z}$. Notationally, we shall often write this as

$$x|y,$$

which should be read 'x divides y', or as 'x is a factor of y'. By our convention we have to say that every integer (including 0) is a divisor of 0.

A number $p \in \mathbf{N}$ is said to be a *prime number* if it is not equal to 1 and if its only divisors are 1 and itself. The first few primes numbers are:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots.$$

1.2 Euclid's Greatest Common Divisor Algorithm

Euclid presents an exposition of number theory in Book VII of the *Elements*. In Proposition 2 of this book, he describes an algorithm for finding the greatest common divisor of two numbers. In this section we will describe Euclid's algorithm.

Quite separately, Euclid also developed, in Book X of the *Elements*, an analogous theory applicable to *magnitudes* (such as line segments or plane areas), as opposed to numbers. We shall discuss this theory in a later section.

In this section, we use the term 'number' to mean a natural number, i.e. a positive integer.

Consider numbers

$$a, b.$$

A *common divisor* of a and b is a number integer which divides both a and b. The *greatest common divisor*, or gcd, of a and b is the largest number which divides both a and b, and is denoted

$$\gcd(a, b).$$

For example,

$$\gcd(45, 63) = 9.$$

We say that a and b are *co-prime* if their gcd is 1. For example, 16 and 21 are co-prime.

Euclid Book VII Proposition 2 describes how to work out the gcd of two numbers (the procedure is believed to have been known in the Greek mathematical community prior to Euclid). The idea is simple, and Euclid states it in one sentence:

> *Subtract the smaller number from the larger repeatedly until the smaller number turns out to be a divisor of the larger; the gcd is the last 'smaller' number.*

This method, and related procedures of reducing a number theoretic problem to one involving smaller numbers, was known in India (around 500 AD in the works of Aryabhatta and others) as the method of 'pulverizing'.

To see this in action, let us work out

$$\gcd(288, 90).$$

Subtracting the smaller from the larger we obtain the following pairs:

288	90	
198	90	
108	90	
18	90	: the process halts here because 18 is a divisor of 90.

We halt the process here on observing that 18 is a divisor of 90. The gcd is 18.

The procedure becomes a little easier to analyze if we change the halt instruction to the following: halt the process when the two numbers become equal, this common value being the gcd. Carrying this out in our example we have:

288	90	
198	90	
108	90	
18	90	
18	72	
18	54	
18	36	
18	18.	:the process halts here because the two values are equal.

A moment's thought shows that there is no real difference between Euclid's prescription and the longer one stated above in terms of the answer that would be produced.

Let us now state the algorithm more formally. Let

$$a \qquad \text{and} \qquad b$$

be the numbers whose gcd is the be found. The following is the procedure:

1. Set
$$a_1 = a \qquad \text{and} \qquad b_1 = b.$$

2. If $a_i \neq b_i$ define the next pair a_{i+1}, b_{i+1}, by:
$$a_{i+1} = \max\{a_i, b_i\} - \min\{a_i, b_i\}$$
$$b_{i+1} = \min\{a_i, b_i\}.$$

3. If $a_i = b_i$ then
$$\gcd(a,b) = b_i,$$
and the process halts.

Note that in step 2, assuming the two numbers at stage i are unequal shows that in the next stage we do again obtain numbers ≥ 1 (the max of a_i, b_i is not equal to their min).

Let us now see why the process will definitely produce the gcd of a and b.

The first question to ask (which was not explicitly done by Euclid) is why this procedure would ever halt. To see why the procedure does halt eventually, observe that at each stage we have numbers a_i and b_i (both ≥ 1), and if they are unequal then in the next stage the larger of the numbers a_i, b_i gets *reduced* by at least 1. Let
$$a = \max\{a,b\}.$$
If the process were to be continued to A number of steps then the resulting numbers would be ≤ 0, which is impossible. Thus the procedure must halt in less than A steps.

Now observe that if a number is a divisor of two numbers then it is certainly also a divisor of their difference. Formally, if $x|a$ and $x|b$ then
$$a = mx \text{ and } b = nx \text{ for some numbers } m \text{ and } n,$$
and so
$$a - b = mx - nx = (m-n)x$$
which shows that x is a divisor of $a - b$.

The preceding observation shows that any common divisor of a_i and b_i would be a common divisor of a_{i+1}, b_{i+1} in the algorithm.

Conversely, observe that
$$a_{i+1} + b_{i+1} = \max\{a_i, b_i\} \text{ and } b_{i+1} = \min\{a_i, b_i\}.$$
Therefore, a common divisor of a_{i+1} and b_{i+1} would be a divisor of a_i and b_i.

Thus, the common divisors of the pairs (a_i, b_i) remain the same as one continues through the algorithm. The final step in the algorithm produces the output
$$c = a_N = b_N.$$
The greatest common divisor of c and c, is, of course, c itself. Thus,
$$\gcd(a,b) = c.$$

Each step in the preceding algorithm used very simple arithmetic operations: picking the smaller of two given numbers, and subtracting the smaller from the larger.

Let us look back at our example:

288	90	
198	90	
108	90	
18	90	
18	72	
18	54	
18	36	
18	18.	:the process halts here because the two values are equal.

Notice that in the first four steps, the number 90 is subtracted from 288 repeatedly, until a smaller number, 18, results. More generally, if A and B are numbers then we can keep subtracting B from A stopping only when the resulting number is smaller than B; thus, we see that A is a multiple of B plus a number smaller than B:

$$A = qB + r$$

where q, r are integers, with

$$0 \leq r < B.$$

Note that if we began with a number B larger than A then the process terminates immediately, produce $q = 0$ and $r = B$. The integer q is the *quotient* on dividing A by B, and r is the *remainder*.

If we use this *division algorithm* as a ‘sub-routine’ in the algorithm then we have a shorter algorithm:

1. Set
$$a_1 = a \qquad \text{and} \qquad b_1 = b.$$

2. If b_i is not a divisor of a_i then divide a_i by b_i, obtaining quotient q and remainder r, and then set
$$a_{i+1} = r \text{ and } b_{i+1} = \min\{a_i, b_i\}.$$

3. If b_i is a divisor of a_i then

$$\gcd(a,b) = b_i,$$

and the process halts.

1.3 Consequences of Euclid's Algorithm

In this section we shall explore some profound results about numbers that follow from applying the Euclidean algorithm.

Examining the algorithm

$$a_{i+1} = \max\{a_i, b_i\} - \min\{a_i, b_i\}, \qquad b_{i+1} = \min\{a_i, b_i\},$$

we see that each number produced at this stage is an integer combination of the preceding two:

$$a_{i+1} = Ea_i + Fb_i, \qquad b_{i+1} = Ga_i + Hb_i,$$

where E, F, G, H are integers (possibly $-1, 0,$ or 1). It follows from this that each of a_i and b_i is an integer linear combination of the original a and b. In particular, going to the very last line, we see that c can be expressed as

$$c = ma + nb,$$

where m and n are integers. Thus,

$$\boxed{\gcd(a,b) = ma + nb \text{ for some integers } m \text{ and } n.} \tag{1.2}$$

It is useful to note that *if d is a common divisor of a and b then d divides any integer linear combination*

$$Ma + Nb, \tag{1.3}$$

because here both Ma and Nb are multiples of d and hence so is the sum.

For example, the greatest common divisor of 45 and 35 is 5, and this can be expressed in terms of 45 and 35 as

$$5 = \underbrace{4 \times 35}_{140} + \underbrace{(-3) \times 45}_{-135}.$$

Now consider three numbers x, y, and z, and suppose z is co-prime to x. Thus,

$$\gcd(z,x) = 1.$$

Let D denote the greatest common divisor of z and y:

$$\gcd(z,y) = D.$$

Our objective is to show that the gcd of z and xy is also D. First note that D is a divisor of z and of xy, because we know that D is a common divisor of z and y. Next we will show that any common divisor of z and xy will also be divisor of D. For this we will show that a relation of the type (1.3) holds for $a = z$ and $b = xy$. To this end we use the fact that there are integers m and n such that

$$mz + nx = 1,$$

and integers s and t such that

$$sz + ty = D.$$

In order to get to the product xy, we multiply the preceding equations together:

$$(mz + nx)(sz + ty) = D.$$

Thus,

$$msz^2 + mtzy + nsxz + ntxy = D.$$

Regrouping terms on the left, this becomes:

$$(msz + mty + nsx)z + (nt)xy = D.$$

Thus, we have established that any common divisor of z and xy is also a divisor of D. We had already noted the converse, that D is a common divisor of z and xy. Thus, D is the greatest common divisor of z and xy.

We summarize these observations:

Proposition 1 *Suppose x, y, and z are numbers.*

(i) If z is co-prime to x then

$$\gcd(z,xy) = \gcd(z,y). \tag{1.4}$$

(ii) If z is co-prime to both x and y then z is co-prime to xy.

(iii) If z is co-prime to x and z is a divisor of xy then z is a divisor of y.

Parts (ii) and (iii) follow from (i). For example, for (iii), if z is co-prime to x and is a divisor of xy then

$$\gcd(z, xy) = z.$$

Consequently, by (i) it follows that

$$\gcd(z, y) = z.$$

But this means that z is a divisor of y.

We can deduce Euclid's Proposition 32 (Book VII) from the preceding result (Euclid's proof uses a different strategy):

Theorem 1 *Every number greater than one is divisible by a prime.*

Suppose there is a number > 1 not divisible by any prime. Then, by the well-ordering principle, there is a least such number; call this x. Since x divides itself, and x has no prime divisor, x cannot be prime. Therefore, x has a divisor y which is neither 1 nor x. In particular, $1 < y < x$. Therefore, y must have a prime divisor p. But then p would also divide x. This contradiction proves the theorem.

Now we can prove that

Theorem 2 *Every number > 1 is a product of primes.*

If this were not so then there would be a least number $x > 1$ not a product of primes. Now we know that x has a prime divisor p. Therefore,

$$x = py,$$

for some number y, and $1 < y < x$. But then y, being a number greater than 1 but less than x, would be a product of primes. But then it would follow that $x = py$ itself would be a product of primes. The contradiction proves the result.

The *Fundamental Theorem of Arithmetic* says:

Theorem 3 *Every number > 1 is a product of primes in a unique way.*

(Though definitely known in Euclid's time, this does not appear explicitly in Euclid's *Elements*.)

For example,

$$240 = 2^4 \times 3 \times 5.$$

It is somewhat complicated to state the uniqueness part in a precise way: *If a number can be expressed as both*

$$p_1^{a_1}...p_r^{a_r},$$

and as

$$q_1^{b_1}...q_s^{b_s},$$

where the p_i*'s are distinct primes in increasing order (*$p_1 < p_2 < \cdots < p_r$*), the* q_i*'s are distinct primes in increasing order, and the* a_i *and* b_j *numbers, then* $r = s$*, and each* $p_i = q_i$*, and each* $a_i = b_i$*.*

The proof of the uniqueness part of the fundamental theorem was presented in class.

Finally, let us look at one of the most celebrated results from Euclid (Proposition 20 of Book IX in the *Elements*):

Theorem 4 *There are infinitely many prime numbers.*

At first it may seem to be impossible to prove such a result: how could one actually produce infinitely many primes? Euclid's argument was by the 'reduction to absurdity' method, i.e. by the the method of contradiction. Suppose in fact there are only finitely many primes, these being

$$p_1,...,p_k.$$

Consider then the number

$$x = 1 + p_1...p_k.$$

If this were divided by p_1 it would leave a remainder of 1. Similarly, x is not divisible by any of the primes p_i. But x is a number > 1, and so *must* have a primes divisor. Thus, we have reached a contradiction.

1.4 Euclid's Algorithm for Magnitudes: The Geometric Viewpoint

In Book X of Euclid's *Elements*, Euclid develops the notion of commensurate and incommensurate *magnitudes*. A magnitude is an abstract entity which measures a geometric object, and, in practice, may refer to length, area of volume.

For definiteness, let us focus on line segments in Euclidean geometry. There is the notion of congruence of two segments. A segment x is greater than a segment y if there are points on x which mark off a segment congruent to y.

A segment x *measures* a segment y if a whole number of copies of x form a segment congruent to y.

The segments x and y are *commensurate* if they have a common measure. (This is essentially Definition I of Book X in the *Elements*.

If m copies of z cover x, and n copies of z cover y, then the formal 'ratio' $x : y$ corresponds to the rational number m/n, and may well be considered good reason for defining the notion of a rational number.

Two magnitudes are *incommensurable* if they are not commensurate. In Proposition 2 of Book X, Euclid lays out his algorithm for finding the *greatest common measure* of two commensurable magnitudes:

Given two magnitudes, continue to subtract the larger from the smaller. If equal magnitudes are obtained at some stage then this is the greatest common measure of the original pair of magnitudes. If equal magnitudes are never obtained then the original magnitudes are incommensurable.

Though structurally identical to the procedure for finding the greatst commond divisor, the contex is quite different, and, furthermore, it leads to the discovery of incommensurable magnitudes. This is the geometric basis for introducing irrational numbers; they are ratios of incommensurable magnitudes.

It should be kept in mind that a segment is not a magnitude. Rather, an equivalence class of all segments congruent to each other is a magnitude. (A similar formulation may be made for planar regions.) However, we have not been and will not be too precise about this distinction.

Suppose q copies of CD can be placed in AB, starting at A, and leaves a segment EB smaller than CD:

$$AB = q \cdot CD + EB.$$

Thus, q is the 'quotient' and EB the remainder. Euclid's algorithm for finding the greatest common measure (which we continue to call *gcd*) works as follows:

1. Draw a rectangle of length x and width y;

2. Mark off on the longer side, say y, as many copies as possible, say q, of the shorter side x, and remove the rectangle thus formed with sides qx by x (this may be done step by step, removing x-by-x squares);

3. If the remaining rectangle, r by x, is not a square, then apply Step 2 to it;

4 If the remaining rectangle at any stage is a square then halt the process; the side of this square is the *greatest common measure* (gcd) of the original segments of length x and y.

If we do start with x and y which are commensurate, say

$$x = mz, \qquad y = nz,$$

then the procedure above is simply that of finding the gcd of m and n and we have seen that the process will halt in at most m steps, and produce the segment

$$gz,$$

where

$$g = \gcd(m,n).$$

Conversely, if the process halts after a finite number of steps then we will have obtained a common measure (indeed the greatest common measure) z of x and y, and so both x and y would be whole multiples of z.

Thus, *if we happen to have x and y for which the Euclid algorithm never halts then $x : y$ is irrational,* which is another way of saying that x and y are incommensurate.

1.5 From Euclid's Algorithm to Continued Fractions

In this section we shall explore further consequences of the geometric form of Euclid's algorithm. However, for practical convenience, we will use standard notation and knowledge about the real number system.

It is possible to rewrite the material below with 1 replaced by any particular magnitude and $\sqrt{2}$ replaced by the diagonal of the square on that segment. The algebraic manipulations could also be replaced by geometric constructs.

We can apply this to $\sqrt{2}$. Consider the rectangle R_0 of height 1 and length $\sqrt{2}$. The first rectangle R_1 we mark off will have side 1 and will leave a remainder of $\sqrt{2}-1$:

$$\sqrt{2} = 1 + (\sqrt{2}-1).$$

Next, we have a rectangle R_2 of sides 1 and $\sqrt{2}-1$. Marking off the largest multiple of $\sqrt{2}-1$ in 1 we have:

$$1 = 1\cdot(\sqrt{2}-1) + 2 - \sqrt{2}.$$

The next rectangle R_3 has sides

$$2-\sqrt{2} \text{ by } \sqrt{2}-1.$$

But here we notice that

$$2-\sqrt{2}=(\sqrt{2}-1)\sqrt{2},$$

and so our rectangle R_3 has sides

$$X \text{ by } X\sqrt{2},$$

where $X=\sqrt{2}-1$. Thus, R_3 is the original rectangle R_0 scaled by the factor X. Then it is clear that as we continue on applying Euclid's algorithm we will keep repeating the sequences

$$R_0, R_1, R_2,$$

with a scaling factor of X applied at each run. Clearly then this process will never halt. Thus, we have proved that $\sqrt{2}$ *is irrational.*

Here is a way to lay out the Euclidean algorithm in this context:

$$\begin{aligned}\sqrt{2} &= 1+(\sqrt{2}-1)\\ &= 1+\frac{1}{\frac{1}{\sqrt{2}-1}}\\ &= 1+\frac{1}{1+\frac{2-\sqrt{2}}{\sqrt{2}-1}}\\ &= 1+\frac{1}{1+\sqrt{2}}\end{aligned} \tag{1.5}$$

You should try out a proof of the irrationality of $\sqrt{3}$ in this way.

Let us now extract the essence of the preceding procedure. Consider positive real numbers x and y. We write the ratio $\frac{x}{y}$ by using the division

$$x=q_0y+r_1,$$

where q_0, the quotient, is a whole number, and $0 \leq r_1 < y$. Then we apply the same to the ratio y/r_1:

$$y=q_1r_1+r_2,$$

and so on, producing

$$\begin{aligned} x &= q_0y + r_1 \\ y &= q_1r_1 + r_2 \\ r_1 &= q_2r_2 + r_3 \\ r_2 &= q_3r_3 + r_4 \\ \vdots &= \vdots \end{aligned}$$

Notice that we can display this also as

$$\begin{aligned} \frac{x}{y} &= q_0 + \frac{r_1}{y} \\ &= q_0 + \frac{1}{\frac{y}{r_1}} \\ &= q_0 + \frac{1}{q_1 + \frac{r_2}{r_1}} \\ &= q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{r_3}{r_2}}} \end{aligned}$$

We know that if the original ratio is rational then this procedure terminates, while if x/y is irrational then the procedure does not terminate.

Given a sequence of numbers $q_0, q_1, ..., q_n$, with q_0 being possibly 0, we can form the *continued fraction*

$$q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \cdots + \frac{1}{q_n}}}, \tag{1.6}$$

which is denoted in short by

$$[q_0; q_1, ..., q_n].$$

Of course, we have seen that an irrational number would generate an infinite continued fraction

$$[q_0; q_1, q_2, ...].$$

Note that by allowing q_0 to range over $\{0, 1, 2, ...\}$ we obtain in this way all real numbers ≥ 0, and by allowing q_0 to be any integer (possibly negative) we are able to obtain any real number.

1.6 Continued Fractions: The Basics

In this section we shall develop the essential facts about continued fractions.

The first objective will be to work out the continued fraction

$$[q_0; q_1, ..., q_n]$$

in the form

$$\frac{P_n}{Q_n} = [q_0; q_1, ..., q_n],$$

with integer P_n and Q_n.

For reasons which will become clear shortly let us introduce the notation

$$P_{-1} = 1, \qquad Q_{-1} = 0.$$

The simplest continued fraction is given by a whole number q_0 itself. We can write this as

$$\frac{P_0}{Q_0} = q_0,$$

with

$$P_0 = q_0, \qquad Q_0 = 1 \tag{1.7}$$

Now that we have (P_{-1}, Q_{-1}) and (P_0, Q_0), we will show that all the numbers P_n and Q_n can be generated by applying a simple recursive scheme:

$$P_{n+1} = q_{n+1}P_n + P_{n-1}, \qquad Q_{n+1} = q_{n+1}Q_n + Q_{n-1}.$$

The proof of this will keep us busy for a page.

Consider, as a first step, the continued fraction

$$[q_0; q_1] = q_0 + \frac{1}{q_1} = \frac{q_1 q_0 + 1}{q_1}. \tag{1.8}$$

The numerator and denominator of the right side are denoted P_1 and Q_1:

$$P_1 = q_1 q_0 + 1, \qquad Q_1 = q_1.$$

Observe that we can write these as:

$$P_1 = q_1 P_0 + P_{-1}, \qquad Q_1 = q_1 Q_0 + Q_{-1}. \tag{1.9}$$

We can move to the next level

$$[q_0; q_1, q_2] = q_0 + \frac{1}{q_1 + \frac{1}{q_2}},$$

by observing that this is readily obtained from (1.8) by replacing q_1 with $q_1 + \frac{1}{q_2}$.

Thus, we can write down

$$[q_0; q_1, q_2] = \frac{\left(q_1 + \frac{1}{q_2}\right) q_0 + 1}{\left(q_1 + \frac{1}{q_2}\right)},$$

and so

$$[q_0; q_1, q_2] = \frac{(q_2 q_1 + 1) q_0 + q_2}{q_2 q_1 + 1} = \frac{q_2(q_1 q_0 + 1) + q_0}{q_2 q_1 + 1}.$$

So we write

$$P_2 = q_2 P_1 + P_0, \qquad Q_2 = q_2 Q_1 + Q_0. \tag{1.10}$$

Now let's move on to the general step. Suppose that we have written

$$[q_0; q_1, \ldots, q_n] = \frac{P_n}{Q_n}, \tag{1.11}$$

where P_n and Q_n are integer linear combinations of the $q_0, \ldots, q_n$, and suppose we have the pattern:

$$P_n = q_n P_{n-1} + P_{n-2}, \qquad Q_n = q_n Q_{n-1} + Q_{n-2}.$$

Then we can get to the next step readily:

$$\begin{aligned} [q_0; q_1, \ldots, q_{n+1}] &= [q_0; q_1, \ldots, q_{n-1}, q_n + \frac{1}{q_{n+1}}] \\ &= \frac{\left(q_n + \frac{1}{q_{n+1}}\right) P_{n-1} + P_{n-2}}{\left(q_n + \frac{1}{q_{n+1}}\right) Q_{n-1} + Q_{n-2}}. \end{aligned} \tag{1.12}$$

Simplifying this as before, we obtain

$$[q_0; q_1, \ldots, q_{n+1}] = \frac{q_{n+1}(q_n P_{n-1} + P_{n-2}) + P_{n-1}}{q_{n+1}(q_n Q_{n-1} + P_{n-2}) + Q_{n-1}},$$

and so indeed we have

$$[q_0; q_1, \dots, q_{n+1}] = \frac{P_{n+1}}{Q_{n+1}},$$

where

$$\boxed{P_{n+1} = q_{n+1}P_n + P_{n-1}, \qquad Q_{n+1} = q_{n+1}Q_n + Q_{n-1}.} \tag{1.13}$$

Thus, there is a simple scheme to generate the value of a finite continued fraction.

Let's look at an example. Let's work out the value of the continued fraction

$$[3; 4, 3, 1, 2].$$

n	q_n	P_n	Q_n
-1		1	0
0	3	3	1
1	4	13	4
2	3	42	13
3	1	55	17
4	2	152	47

So the convergents of $[3; 4, 3, 1, 2]$ are

$$3, \frac{13}{4}, \frac{42}{13}, \frac{55}{17}, \frac{152}{47}.$$

Note that

$$P_{n+1} \geq P_n + P_{n-1}, \qquad \text{and} \qquad Q_{n+1} \geq Q_n + Q_{n-1}. \tag{1.14}$$

In particular each P_n exceeds the preceding by at least 1, and so P_n is at least n. The same holds for Q_n. Thus

$$P_n \geq n, \qquad Q_n \geq n. \tag{1.15}$$

(A little thought here shows that these lower bounds are really cheap ones. Indeed, in view of (1.14), one would guess that the P_n and Q_n have lower bounds related to the Fibonacci numbers.)

How much do P_n/Q_n and P_{n+1}/Q_{n+1} differ? To this end we have

$$\frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n} = \frac{P_{n+1}Q_n - P_nQ_{n+1}}{Q_nQ_{n+1}} = \frac{h_{n+1}}{Q_nQ_{n+1}}, \tag{1.16}$$

where h_k denotes the numerator:

$$h_k = P_k Q_{k-1} - P_{k-1} Q_k,$$

which we can develop a step further:

$$\begin{aligned} h_k &= (q_k P_{k-1} + P_{k-2}) Q_{k-1} - P_{k-1}(q_k Q_{k-1} + Q_{k-2}) \\ &= P_{k-2} Q_{k-1} - P_{k-1} Q_{k-2} \\ &= -\Big(P_{k-1} Q_{k-2} - P_{k-2} Q_{k-1} \Big) \\ &= -h_{k-1}. \end{aligned}$$

Thus, each time we reduce the subscript of h_k by 1 we pick up a factor of (-1). So

$$h_k = (-1)^k h_0.$$

Recalling the initial values of P and Q, we have

$$h_0 = P_0 Q_{-1} - P_{-1} Q_0 = q_0 \cdot 0 - 1 \cdot 1 = -1.$$

So

$$h_k = (-1)^k (-1) = (-1)^{k+1}.$$

In other words,

$$\boxed{P_k Q_{k-1} - P_{k-1} Q_k = (-1)^{k+1}.} \tag{1.17}$$

Consequently,

$$\boxed{\frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n} = \frac{(-1)^n}{Q_n Q_{n+1}}.} \tag{1.18}$$

The difference between successive ratios P_n/Q_n is thus

$$\frac{1}{Q_n Q_{n+1}}.$$

As n increases the denominator here, $Q_n Q_{n+1}$, also increases, and so *the difference between successive ratios P_n/Q_n decreases.*

Recall that $Q_n \geq n$, and $Q_{n+1} \geq n+1$. So

$$\left|\frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n}\right| \leq \frac{1}{n^2}. \tag{1.19}$$

The relation (1.18) also shows that

$$\frac{P_1}{Q_1} = \frac{P_0}{Q_0} + \frac{1}{Q_0 Q_1} > \frac{P_0}{Q_0}.$$

Again, similarly,

$$\frac{P_2}{Q_2} < \frac{P_1}{Q_1},$$

and

$$\frac{P_3}{Q_3} > \frac{P_2}{Q_2}.$$

Putting everything together we have

$$\frac{P_0}{Q_0} < \frac{P_2}{Q_2} < \frac{P_4}{Q_4} \cdots < \cdots \frac{P_3}{Q_3} < \frac{P_1}{Q_1}.$$

Suppose now that we take an infinite sequence $q_0, q_1, q_2, \ldots$. Given that successive ratios P_n/Q_n differ by $1/n^2$, there is a unique real number x that lies between all the odd-ratios and the even-ratios:

$$\frac{P_0}{Q_0} < \frac{P_2}{Q_2} < \frac{P_4}{Q_4} \cdots < x < \cdots \frac{P_3}{Q_3} < \frac{P_1}{Q_1}. \tag{1.20}$$

We have

$$\left|x - \frac{P_n}{Q_n}\right| < \frac{1}{n^2}. \tag{1.21}$$

This real number x is denoted as an infinite continued fraction:

$$x = [q_0; q_1, q_2, \ldots], \tag{1.22}$$

and the continued fraction

$$\frac{P_n}{Q_n} = [q_0; q_1, \ldots, q_n]$$

is called the *n–th convergent* to x.

Using what we know about the differences between successive convergents, we can write

$$[q_0; q_1, q_2, \ldots] = q_0 + \frac{1}{Q_1} - \frac{1}{Q_1 Q_2} + \frac{1}{Q_2 Q_3} - \cdots \tag{1.23}$$

1.7 Pell's Equation

Let D be a number which is not a perfect square (for instance, D could be 2). The equation

$$x^2 - Dy^2 = 1 \tag{1.24}$$

is called *Pell's equation.* The name comes the English mathematician Pell (17th century); Euler (apparently mistakenly) credited Pell for a study of this equation, and the name has stuck. The task is to find integers x and y satisfying (1.24).

The simplest case of Pell's equation is with $D = 2$:

$$x^2 - 2y^2 = 1. \tag{1.25}$$

Note that if x and y satisfy the Pell equation (1.24) then

$$\frac{x^2}{y^2} = D + \frac{1}{y^2},$$

and so, if y is a large number, then

$$\frac{x}{y} \approx \sqrt{D}.$$

Thus solutions of Pell's equation with large denominators provide rational approximations to the irrational number $\sqrt{D}$.

A solution of Pell's equation appears implicitly in one of the *Sulva Sutras* authored by Baudhayana (approx. 800 BC; but these dates are not always trustworthy, with some dating Baudhayana to around 400 BC). In describing the construction of an altar, the following approximate value of $\sqrt{2}$ is given:

$$\sqrt{2} \simeq 1 + \frac{1}{3} + \frac{1}{3\times 4} - \frac{1}{3\times 4\times 34} = \frac{577}{408}.$$

As we can check,

$$577^2 - 2(408)^2 = 1.$$

In fact, even the first three terms of Baudhayana give

$$1 + \frac{1}{3} + \frac{1}{3\times 4} = \frac{17}{12},$$

and we can check that

$$17^2 - 2(12)^2 = 1.$$

For $\sqrt{3}$, Baudhayana provides the prescription

$$\sqrt{3} = 1 + \frac{2}{3} + \frac{1}{3\times 5} - \frac{1}{3\times 5\times 52} = \frac{1351}{780},$$

which again provides solutions to the Pell equation with $D = 3$.

Approximations to $\sqrt{3}$ providing solutions to Pell's equation were also given by Archimedes (287-212 BC). But a more celebrated example is the the *Cattle Problem* posed by Archimedes. Stated through a complex set of conditions, the problem comes down to finding integers x and y satisfying

$$x^2 - 4729494y^2 = 1.$$

According to Archimedes,

> *If thou art able, O stranger, to find out all these things and gather them together in your mind, giving all the relations, thou shalt depart crowned with glory and knowing that thou hast been adjudged perfect in this species of wisdom.*

It was shown by Amthor (1880) that the smallest solution has over twenty thousand digits in decimal form. For a visual representation of the solution see the illustration

http://www.ams.org/notices/200202/noti-feb02-cov.jpg
for Lenstra's article
http://www.ams.org/notices/200202/fea-lenstra.pdf
in the American Mathematical Society Notices.

A clear algorithm for solving Pell's equation was stated by Euler (1770) using the Euclidean algorithm (called the continued fraction method). Lagrange (1768) published a proof showing that the continued fraction method always works, confirming a claim made earlier by Fermat.

Let D be a number which is not a perfect square. Lagrange proved that the continued fraction for $\sqrt{D}$ is periodic after a certain point. Let us take the simple case in which the number

$$Z = \sqrt{D}$$

has a periodic continued fraction expression as

$$Z = [q_0; q_1, ..., q_n, Z].$$

Then

$$Z = \frac{P_{n+1}}{Q_{n+1}} = \frac{ZP_n + P_{n-1}}{ZQ_n + Q_{n-1}},$$

which implies:

$$DQ_n + Q_{n-1}\sqrt{D} = P_n\sqrt{D} + P_{n-1}.$$

Bringing the rationals to one side and the irrationals to the other we have

$$DQ_n - P_{n-1} = (P_n - Q_{n-1})\sqrt{D}.$$

Since a rational cannot be equal to an irrational, we conclude that

$$P_n = Q_{n-1}, \qquad \text{and} \qquad P_{n-1} = DQ_n.$$

We substitute these into the identity

$$P_nQ_{n-1} - P_{n-1}Q_n = (-1)^{n+1},$$

to obtain

$$P_n^2 - DQ_n^2 = (-1)^{n+1}.$$

If n is odd then we have a solution to the Pell equation

$$x^2 - Dy^2 = 1,$$

on taking $x = P_n$ and $y = Q_n$.

1.8 Solving Equations Using Continued Fractions

Consider a continued fraction

$$[q_0; q_1, q_2, \ldots].$$

Let P_n and Q_n be as before, with

$$\frac{P_n}{Q_n} = [q_0; q_1, \ldots, q_n].$$

Recall the fundamental identity (we saw this in (1.17)):

$$P_nQ_{n-1} - P_{n-1}Q_n = (-1)^{n+1}. \tag{1.26}$$

Observe that this implies that the gcd of P_n and Q_n is 1: for if c is a number which divides both P_n and Q_n then the left side of (1.26) would be a multiple of c, which would imply that c is a divisor of 1, and hence that c *is* 1.

Thus,

$$\gcd(P_n, Q_n) = 1. \tag{1.27}$$

Thus, the ratio

$$\frac{P_n}{Q_n}$$

has no common factor between numerator and denominator (other than 1). Thus, for example if we develop the rational number

$$\frac{28}{35}$$

in a continued fraction:

$$\begin{aligned}\frac{28}{35} &= 0 + \frac{1}{\frac{35}{28}} \\ &= 0 + \frac{1}{1 + \frac{7}{28}} \\ &= 0 + \frac{1}{1 + \frac{1}{4}}.\end{aligned}$$

Thus,

$$\frac{28}{35} = [0; 1, 4].$$

The intermediate continued fractions are

$$0, [0; 1], \text{and}\, [0; 1, 4].$$

The values are:

$$0, 1, 0 + \frac{1}{1 + \frac{1}{4}} = \frac{4}{5}.$$

Note that the continued fraction convergent produced at the end is

$$\frac{4}{5}$$

in place of the original

$$\frac{28}{35}.$$

This is because, as we have seen,

$$\frac{P_n}{Q_n}$$

has no common factor between numerator and denominator (other than 1).

There is more provided by the relation (1.26):

$$P_nQ_{n-1} - P_{n-1}Q_n = (-1)^{n+1}.$$

It provides numbers x and y which solve the equation

$$P_nx - Q_ny = 1,$$

if n is odd, with

$$x = Q_{n-1}, \qquad \text{and} \qquad y = P_{n-1}.$$

If n is even we can move a step further, and using the same relation with $n+1$ in place of n, we have

$$P_{n+1}Q_n - P_nQ_{n+1} = (-1)^{n+2}.$$

As an example, let us find x and y solving

$$152x - 47y = 1.$$

Let us work out the continued fraction for $152/47$:

$$\begin{aligned}
\frac{152}{47} &= 3 + \frac{11}{47} \\
&= 3 + \frac{1}{47/11} \\
&= 3 + \frac{1}{4 + \frac{3}{11}} \\
&= 3 + \frac{1}{4 + \frac{1}{3 + \frac{2}{3}}} \\
&= 3 + \frac{1}{4 + \frac{1}{3 + \frac{1}{1 + \frac{1}{2}}}} = [3; 4, 3, 1, 2] \\
&= 3 + \frac{1}{4 + \frac{1}{3 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1}}}}} = [3; 4, 3, 1, 1, 1].
\end{aligned}$$

Note that, as is true for every rational, we can terminate the continued fraction in either an odd number of steps or an even number.

Let us work out the continued fractions leading to $[3; 4, 3, 1, 1, 1]$:

n	q_n	P_n	Q_n
-1		1	0
0	3	3	1
1	4	13	4
2	3	42	13
3	1	55	17
4	1	97	30
5	1	152	47

From the general theory we know that

$$Q_{n-1}P_n - P_{n-1}Q_n = (-1)^{n-1}.$$

Let's take this with $n = 5$. Then we have:

$$(30 \times 152) - (97 \times 47) = (-1)^{5-1} = 1.$$

Thus we have a solution to

$$152x - 47y = 1,$$

with

$$x = 30, y = 97.$$

1.9 Fibonacci Numbers and Euclid's Algorithm

Consider the *simplest* continued fraction:

$$[1;1,1,1,....] = 1 + \frac{1}{1+\frac{1}{1+\vdots}}.$$

Let us work out the values of P_n and Q_n in this case.

Recall the fundamental relations by which P_n and Q_n are generated:

$$P_n = q_n P_{n-1} + P_{n-2}$$
$$Q_n = q_n Q_{n-1} + Q_{n-2},$$

starting with the initial values

$$P_{-1} = 1 \qquad Q_{-1} = 0$$
$$P_0 = q_0 \qquad Q_0 = 1.$$

We are working now with

$$[1;\underbrace{1,1,...,1}_{n}] = \frac{P_n}{Q_n},$$

and so

all the q_n are 1.

Consequently,

$$\begin{aligned} P_n &= P_{n-1} + P_{n-2} \\ Q_n &= Q_{n-1} + Q_{n-2}, \end{aligned}$$

Each Q_n is the sum of the preceding two, beginning with the initial values 0 and 1. Thus, *the* Q_n *form the Fibonacci sequence*:

$$F_{-1} = 0, F_0 = 1, F_1 = 1, F_2 = 2, F_3 = 3, F_4 = 5, \ldots.$$

So

$$Q_n = F_n.$$

For the P_n we have the same relation, that each term is the sum of the preceding two, but the initial values are

$$P_{-1} = 1, P_0 = 1,$$

which match with

$$F_0 = 1, F_1 = 1.$$

Consequently,

$$P_n = F_{n+1}.$$

Thus,

$$\frac{P_n}{Q_n} = \frac{F_{n+1}}{F_n},$$

and so

$$[1;\underbrace{1,...,1}_{n}] = \frac{F_{n+1}}{F_n}. \tag{1.28}$$

We know that the infinite continued fraction

$$[1;1,1,1,...]$$

is the limit

$$\lim_{n\to\infty}[1;\underbrace{1,...,1}_{n}].$$

Thus, we have

$$\boxed{\lim_{k\to\infty}\frac{F_{k+1}}{F_k}=[1;1,1,1,...].} \tag{1.29}$$

This number is called the *Golden Ratio*, and often denoted by ϕ.

Recalling the geometric representation of the Euclidean algorithm, we see that if we form a rectangle whose sides are ϕ and 1, and apply the geometric Euclid algorithm then we will produce a succession of rectangles, each proportional to the original one.

By visual inspection of the continued fraction:

$$\boxed{\phi=1+\frac{1}{1+\frac{1}{1+\frac{1}{\vdots}}},} \tag{1.30}$$

it is clear that

$$\phi=1+\frac{1}{\phi}. \tag{1.31}$$

However, to be sure, this isn't a real proof of this equation, because the $\vdots$ in (1.30) are just a picturesque way of expressing the real definition of ϕ, which is the limit given in (1.29).

But let us proceed with (1.31) for now. Then

$$\phi^2=\phi+1,$$

and so

$$\phi^2-\phi-1=0.$$

Solving this quadratic equation we get

$$\phi=\frac{1\pm\sqrt{1+4}}{2}=\frac{1\pm\sqrt{5}}{2}.$$

Now ϕ is clearly positive, and so we have

$$\boxed{\phi=\frac{1+\sqrt{5}}{2}.} \tag{1.32}$$

Now let us prove (1.31). We have

$$\begin{aligned}\phi &= \lim_{n\to\infty}\frac{F_{n+1}}{F_n}\\ &= \lim_{n\to\infty}\frac{F_n+F_{n-1}}{F_n}\\ &= \lim_{n\to\infty}\left(1+\frac{F_{n-1}}{F_n}\right)\\ &= 1+\lim_{n\to\infty}\frac{1}{F_n/F_{n-1}}\\ &= 1+\frac{1}{\phi}.\end{aligned}$$

Thus,

$$\phi = 1+\frac{1}{\phi}.$$

1.10 Continued Fractions: A Working Scheme

We will develop a scheme for working out the quantities q_n, P_n, Q_n for a given positive real number T developed as a continued fraction.

Suppose

$$T = [q_0; q_1, ..., q_{n1}, x],$$

where $q_0, q_1, ..., q_n$ the usual quotients, and x is a positive real number. Then

$$q_{n+1} = [x],$$

the integer part of x. Now we have

$$T = \frac{xP_n + P_{n-1}}{xQ_n + Q_{n-1}} \tag{1.33}$$

Solving for x we obtain:

$$x = -\frac{TQ_{n-1} - P_{n-1}}{TQ_n - P_n}.$$

Recall that

$$q_{n+1} = [x], \tag{1.34}$$

the integer part of x.

Take the case where T is a rational:

$$T = \frac{A}{B},$$

where A and B are numbers. Then the expression of x can be rewritten as

$$x = -\frac{AQ_{n-1} - BP_{n-1}}{AQ_n - BP_n}. \tag{1.35}$$

Let us write

$$d_n = AQ_n - BP_n.$$

Then we can form a table using the scheme:

		A	B	
n	q_n	P_n	Q_n	d_n
-1		1	0	$A \cdot 0 - B \cdot 1 = -B$
0	$q_0 = [A/B]$	q_0	1	$A \cdot 1 - Bq_0$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
k	$q_k = [-d_{k-2}/d_{k-1}]$	$P_k = q_k P_{k-1} + P_{k-2}$	$Q_k = q_k Q_{k-1} + Q_{k-2}$	$AQ_k - BP_k$

Let us implement this for

$$\frac{25}{14}.$$

We have:

		$A = 25$	$B = 14$	
n	q_n	P_n	Q_n	d_n
-1		1	0	-14
0	$q_0 = [25/14] = 1$	1	1	11
1	$q_1 = [14/11] = 1$	2	1	-3
2	3	7	4	2
2	1	9	5	-1
3	2	25	14	0

Notice how the numbers down the last column alternate in sign but decrease in magnitude.

Reading down the first column, we have

$$\frac{25}{14} = [1; 1, 3, 1, 2].$$

From the penultimate row we see that

$$(25\times 5)-(14\times 9)=-1.$$

Thus, if are to solve the equation

$$25x+14y=1 \tag{1.36}$$

in *integers* x and y we obtain

$$x=-5, y=9.$$

We can obtain other solutions of (1.36) by a simple trick:

$$x=-5+14k, \qquad y=9-25k, \tag{1.37}$$

for any integer k. We can see then

$$\begin{aligned}25(-5+14k)+14(9-25k)&=25(-5)+14(9)+(25\times 14k)-(14\times 25k)\\&=25(-5)+14(9)\\&=1.\end{aligned}$$

As shown in class, (1.37) provides *all* solutions of the equation (1.36).

Problem Sets 1 and 2

1. Let p_j denote the j-th prime. Thus,

   $$p_1=2, p_2=3, p_3=5, \ldots.$$

   Show that

   $$p_{k+1}\leq p_1 \ldots p_k-1,$$

   for every $k\in\{2,\ldots\}$.

2. With notation as in the preceding problem, produce primes $p_1,\ldots,p_j$ for which $1+p_1\ldots p_j$ is *not* a prime.

3. Here is another proof that there are infinitely many primes (really, just a take-off on Euclid's idea, but used much later by others such as Goldbach (1730)). *Let a and b be co-prime numbers, both* > 1 (for example, $a = 2$ and $b = 5$). Consider the sequence of numbers given as follows

$$x_1 = a,$$

$$x_2 = a + b,$$

$$x_3 = x_2 x_1 + b,$$

$$x_4 = x_3 x_2 x_1 + b,$$

   and so on, with x_{n+1} being the product $x_1 ... x_n$ plus b. Note that x_n's keep increasing, i.e. $x_{n+1} > x_n$ for each n.

   (i) Show that x_1 is co-prime to all the other x_n (Hint: If y divides both x_1 and x_n then show that y must divide b; now recall that x_1 is actually a).

   (ii) Show that $\gcd(x_2, b) = 1$.

   (iii) Show that x_2 is co-prime to all other x_n.

   (iv) Show that x_3 is co-prime to b (Hint: Look at $x_3 = x_1 x_2 + b$, and use (i) and (iii), i.e. that x_3 is co-prime to both x_1 and x_2.]

   (v) Show that x_n and x_m are co-prime for $n \neq m$.

   (vi) Prove that there are infinitely many primes. [Hint: Use the fact that each x_n has a prime divisor.]

4. A number is said to be *square-free* if it has no divisor, other than 1, which is a square; thus, for example, 30 is square-free (its divisors, other than 1, are $2, 3, 5, 6, 10, 15, 30$, none of which is a square), but 48 is not square-free since it has, for instance, $16 = 4^2$ as divisor. The first few-square numbers are:

$$1, 2, 3, 5, 6, 7, 10.$$

   (i) Show that the number of square-free numbers which are divisible by at most the first four primes (i.e. 2, 3, 5, and 7) is 2^4. [Hint: In such a number each of the first four primes can either appear as a factor or not appear as a factor.] Use this idea to show that there are 2^k square-free numbers having at most the first k primes as divisors.

(ii) Show that every number x can be expressed in the form

$$x = ab^2,$$

where a and b are numbers and a is square-free.

(iii) Let p_j denote the j-th primes; thus, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, etc. Prove the inequality

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{N} \leq \left(1+\frac{1}{p_1}\right)\left(1+\frac{1}{p_2}\right)\cdots\left(1+\frac{1}{p_{N'}}\right)\sum_{b=1}^{N}\frac{1}{b^2}, \tag{1.38}$$

where $p_{N'}$ is the largest prime $\leq N$. [Hint: Show that the right side can be expanded as a sum of terms each of which is of the form $\frac{1}{ab^2}$, where a is square-free, and both a and b are $\leq N$.]

5. Suppose D is a number with a rational square-root $\sqrt{D}$. Show that D must be a perfect square, i.e. the square of a natural number. [Hint: Suppose $\sqrt{D}$ is rational. Then $D = (m/n)^2$, for some numbers m and n. By canceling common factors, we may assume that m and n have no factor in common. Show that this implies that m^2 and n^2 are also coprime. Now

$$m^2 = Dn^2.$$

Thus m^2 divides the product of D and n^2 and is co-prime to n^2. Conclude, by Proposition 1 (iii), that m^2 divides D. But D also divides m^2.]

6. Suppose x, y, and z are numbers such that

$$x^2 + y^2 = z^2.$$

The goal of this problem is to obtain the complete solution to this. In fact we will show that there are numbers u and v such that

$$x = (u^2 - v^2)c, \quad y = 2uvc, \qquad z = (u^2 + v^2)c,$$

for some number c. This formula for generating Pythagorean triples is given in Euclid Book X, Proposition 29 (Lemma).

(i) If any two of the numbers x, y, z have a common divisor d, then d would also divide the third number.

In view of (i), we can divide through by $\gcd(x, y, z)$ and may and will assume that the numbers x, y, z are pairwise co-prime.

(ii) Check that for any number n, the square n^2, when divided by 4, leaves a remainder of 1 if n is odd, and a remainder of 0 if n is even.

(iii) Apply (ii) to show that one of the numbers x and y must be even, the other one odd, and z is also odd. (Recall that we are assuming that these numbers are mutually co-prime.) Just to be definite, let's say y is even; then x and z are odd.

(iv) Check that

$$\left(\frac{y}{2}\right)^2 = \left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right).$$

Let

$$a = \frac{z+x}{2} \qquad \text{and} \qquad b = \frac{z-x}{2}.$$

Explain why each term $y/2$ and a, b is an integer.

(v) Show that $\gcd(a,b) = 1$. [Hint: $z = a+b$ and $x = a-b$.]

(vi) Explain why a and b are perfect squares, i.e.

$$a = u^2 \qquad \text{and} \qquad b = v^2,$$

for some positive integers u and v.

(vii) Show that

$$y = 2uv.$$

(viii) Show that

$$x = u^2 - v^2 \qquad \text{and} \qquad z = u^2 + v^2.$$

7. Here is another solution to the Pythagorean-triples problem, following ideas of Diophantus (around 200 AD).

(i) On the unit circle

$$x^2 + y^2 = 1,$$

consider the point $(-1,0)$, and suppose (a,b) is *another* point on this circle. Thus,

$$a^2 + b^2 = 1. \tag{1.39}$$

Consider the straight line through $(-1,0)$ and (a,b). Its slope is

$$m = \frac{b-0}{a-(-1)} = \frac{b}{a+1}.$$

The equation of the line is

$$y = m(x+1).$$

Thus,

$$b = m(a+1).$$

Substitute this into (from (1.39))

$$b^2 = 1 - a^2,$$

and show that

$$a = \frac{1-m^2}{1+m^2}.$$

[Hint: $1 - a^2 = (1-a)(1+a)$, and recall that, by assumption, $a \neq -1$.]

(ii) Conclude that if

$$a^2 + b^2 = 1,$$

where $(a,b) \neq (-1,0)$, then

$$a = \frac{1-m^2}{1+m^2} \qquad b = \frac{2m}{m^2+1},$$

where

$$m = \frac{b}{a+1}.$$

(iii) Show that a point (a,b), other than $(-1,0)$, on the unit circle has *rational coordinates* if and only if

$$a = \frac{u^2-v^2}{u^2+v^2} \qquad b = \frac{2uv}{u^2+v^2},$$

for some integers u and v. (Note that we can cancel any common factors and make u and v be co-prime in the end.)

(iv) Now show that if x, y and z are positive integers satisfying

$$x^2 + y^2 = z^2,$$

then there are integers u, v (these being co-prime), and c, such that

$$x = (u^2 - v^2)c, \qquad y = 2uvc, \qquad z = (u^2 + v^2)c.$$

[Hint: If you use (iii) and figure out c, it works out to be $z/(u^2+v^2)$. But it is difficult to see why this should be an integer. Write c as m/n, where m and n are co-prime numbers. Then n is a divisor of both u^2+v^2 and u^2-v^2, and so of both $2u^2 = (u^2+v^2)+(u^2-v^2)$ and $2v^2 = (u^2+v^2)-(u^2-v^2)$. Since u and v are co-prime, it follows that n is a divisor of 2. If $n=1$ we are done. The only other possibility is $n=2$.]

(v) Suppose (x_1,y_1) and (x_2,y_2) are points on the unit circle. Show that the 'product' point

$$(x,y) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$$

is also on the unit circle.

8. Work out the continued fractions for:

(i) $\frac{577}{408}$

(ii) $\sqrt{3}$.

9. Develop $\frac{3141}{1000}$ in a continued fraction. Use the following scheme:

		$A=3141$	$B=1000$	
n	q_n	P_n	Q_n	d_n
-1		1	0	-1000
0	$q_0 = [3141/1000] = 3$	3	1	141
1				
2				
3				
4				

10. Find integers x and y such that

$$3141x + 1000y = 1.$$

11. Find a number x such that when x is divided by 5 it leaves a remainder of 3, when x is divided by 3 it leaves a remainder of 2, and when x is divided by 7 it leaves a remainder of 1.

12. State the continued fraction form of the Golden Ratio. Draw rectangles to illustrate why the Golden Ratio is irrational.

13. Explain why the Golden Ratio ϕ can be expressed as a series:

$$1+\frac{1}{1}-\frac{1}{1\times 2}+\frac{1}{2\times 3}-\frac{1}{3\times 5}+\frac{1}{5\times 8}-\frac{1}{8\times 13}+\cdots$$

    (Hard.)

14. Prove that the Golden Ratio ϕ is a solution of the equation

$$x=1+\frac{1}{x}.$$

15. Show that in a regular pentagon the ratio of the diagonal to any one side is ϕ.

16. Look up Euclid's construction in Proposition 11 (Book 2) at

    http://aleph0.clarku.edu/~djoyce/java/elements/bookII/propII11.html

    and explain how this involves the Golden Ratio.

17. Look through Euclid's elements at

    http://aleph0.clarku.edu/~djoyce/java/elements/toc.html

    and state which result describes the construction of the icosahedron.

Chapter 2

Topics from the Theory of Equations

In this chapter we will study properties of polynomials and some theoretical results on solutions of polynomial equations.

In this version of the notes, methods of solving equations, such as the cubic and quartic equations, are not covered.

2.1 Polynomials in One Variable

An example of a *polynomial* in a symbol X is an expression of the form

$$4X^{18} - 3X^7 + 2X - 5$$

In this case, the coefficients $4, 0, -3, 2, -5$ are all integers. In general we can draw the coefficients also from some other system, such as the rationals or real numbers or complex numbers. The *degree* of the preceding polynomal is 18.

More generally, a polynomial in X is an expression of the form

$$p(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0,$$

where the *coefficients* $a_0, ..., a_n$ are drawn from system of letters or numbers; if $a_n \neq 0$ then we say that $p(X)$ has degree n.

The polynomial 0 is a bit problematic when it comes to the notion of degree. We could leave it undefined or define it to be $-\infty$.

Note that even $-X+4$ is called a polynomial, and so is the constant 4. A constant k is a polynomial of degree 0 (unless that constant k itself if 0).

Multiplying a cubic polynomial with a quadratic gives a fifth degree polynomial. More generally,

$$\deg(p(X)q(X)) = \deg p(X) + \deg q(X).$$

The set of all polynomials in X with integer coefficients is denoted

$$\mathbf{Z}[X].$$

If we allow the coefficients to be rational, the set of such polynomials is denoted

$$\mathbf{Q}[X].$$

In this manner,

$$\mathbf{R}[X] \text{ is the set of all polynomials with real coefficients,}$$

and

$$\mathbf{C}[X] \text{ is the set of all polynomials with complex coefficients.}$$

Polynomials can be added and multiplied to yield polynomials. However, the only polynomials in $\mathbf{Q}[X]$ which have reciprocals (which are polynomials) are the non-zero constants. In $\mathbf{Z}[X]$ the only polynomials with inverses (in $\mathbf{Z}[X]$) are the constants 1 and -1.

If we work inside $\mathbf{Z}[X]$ then many things need to be handled with care, and results for $\mathbf{Z}[X]$ will be pointed out separately.

Consider the polynomial

$$r(X) = \frac{10}{3}x^5 - \frac{25}{6}x + \frac{15}{4}.$$

We can rewrite this in the form

$$r(X) = \frac{5}{12}(8x^5 - 10x + 9).$$

More generally, we can express any polynomial $p(X)$ in $\mathbf{Q}[X]$ in the form

$$p(X) = c_p(a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0),$$

where c_p is rational, and the coefficients $a_0, ..., a_n$ are integers with gcd equal to 1.

2.2 The Division Algorithm for Polynomials

Our main concern here will be with dividing a polynomial by another. Let us look at a simple example:

$$a(X) = 4X^5 - 3X + 6, \quad b(X) = X^2 - 2X + 3$$

One this is clear: we should start out the quotient with $4X^3$. To this end we have

$$\begin{aligned} a(X) - 4X^3 b(X) &= 4X^5 - 3X + 6 - 4X^5 + 8X^4 - 12X^3 \\ &= 8X^4 - 12X^3 - 3X + 6 \end{aligned}$$

So:

$$a(X) = 4X^3 b(X) + 8X^4 - 12X^3 - 3X + 6.$$

But it would be odd to regard $8X^4 - 12X^3 - 3X + 6$ as the 'remainder' from the division, because it is more complex than the divisor $b(X)$. More precisely, it has degree 4, whereas $b(X)$ has only degree 2, so it doesn't seem right to regard $8X^4 - 12X^3 - 3X + 6$ as the 'remainder'. The point is that we can make $b(X)$ go into $8X^4 - 12X^3 - 3X + 6$ again: to match the highest degree term, we multiply $b(X)$ by $8X^2$ and this would leave over

$$\begin{aligned} 8X^4 - 12X^3 - 3X + 6 - 8X^2 b(X) &= 8X^4 - 12X^3 - 3X + 6 - 8X^4 + 16X^3 - 24X^2 \\ &= 4X^3 - 24X^2 - 3X + 6. \end{aligned}$$

Putting together the preceding calculations we have

$$a(X) = (4X^3 + 8X^2)b(X) + 4X^3 - 24X^2 - 3X + 6, \tag{2.1}$$

but we still need to divide the 'remainder' term here by $b(X)$. To match the highest degree term we multiply $b(X)$ by $4X$, and left over piece is

$$\begin{aligned} 4X^3 - 24X^2 - 3X + 6 - 4Xb(X) &= 4X^3 - 24X^2 - 3X + 6 - 4X^3 + 8X^2 - 12X \\ &= -16X^2 - 15X + 6. \end{aligned}$$

So

$$a(X) = (4X^3 + 8X^2 + 4X)b(X) - 16X^2 - 15X + 6, \tag{2.2}$$

which leaves just one more step to cut down the degree of the remainder: we should multiply $b(X)$ by -16 to match the X^2 term and be left over with

$$-16X^2 - 15X + 6 - (-16b(X)) = -47X + 54.$$

Thus, we finally have

$$a(X) = (4X^3 + 8X^2 + 4X - 16)b(X) + (-47X + 54) \tag{2.3}$$

and this gives us the quotient and remainder as

$$q(X) = 4X^3 + 8X^2 + 4X - 16, \qquad r(X) = -47X + 54.$$

Although it is a long process, the method is simple and clear. It is possible to write a program to exceute this process. It is also possible to be braver and just do all the calculations in one non-stop chain, obtaining the quotient and remainder. There are several other ways to organize the computation.

For us the main point to note is that the *division algorithm* works : if $a(X)$ by $b(X)$ are polynomials, with $b(X)$ not being the 0 polynomial, then there are polynomials $q(X)$ and $r(X)$ such that

$$a(X) = q(X)b(X) + r(X),$$

and the degree of $r(X)$ is less than the degree of $b(X)$. In the event that $b(X)$ is a divisor of $a(X)$, the remainder is 0.

Note that the coefficients in $q(X)$ and $r(X)$ are obtained by addition, subtraction, multiplication, and division starting with the coefficients of $a(X)$ and $b(X)$.

2.3 The Greatest Common Divisor for Polynomials

Now that we know that the division algorithm works, we can conclude immediately that any two non-zero polynomials have a *greatest common divisor*, and that this is obtained by the ‘pulverizing’ algorithm of repeatedly dividing and taking the remainder, with the last non-zero remainder being the gcd.

In doing a gcd calculation it is best to keep in mind that for polynomials, if $p(X)$ is a divisor of $q(X)$ then any constant multiple is a divisor of any constant multiple of $q(X)$ (the answer just gets multiplied by a constant). Thus, we can multiply out by constants to avoid nasty fractions. You can multiply the gcd by any constant and it will still be a gcd.

Let us work out

$$\gcd\bigl(a(X), b(X)\bigr),$$

where

$$a(X) = 4X^5 - 3X + 6, \quad b(X) = X^2 - 2X + 3.$$

We have already done the long calculation for the first divison:

$$a(X) = q(X)b(X) + (-47X + 54).$$

Next we need to divide $b(X)$ by $-47X + 54$. To avoid some, but not all, ugly fractions, let's just divide $-47b(X)$ by $-47X + 54$. We have then

$$\begin{aligned} -47X^2 + 94X - 141 &= (-47X + 54)X + +40X - 141 \\ &= (-47X + 54)X + \big(-47X + 54\big)\frac{40}{-47} + \frac{54 \times 40}{47} - 141. \end{aligned} \tag{2.4}$$

Thus, the remainder is the constant

$$\frac{54 \times 40}{47} - 141.$$

There is no point in working this out, for it just suffices to check that it isn't 0. The main thing is that it is a non-zero constant, and so it is certainly a divisor of any polynomial. Thus,

$$\gcd\big(a(X), b(X)\big) = 1.$$

Borrowing terminology from numbers we can say that the polynomials $a(X)$ and $b(X)$ are *co-prime*.

Just as with numbers, the Euclidean algorithm can be used to express the gcd as a combination of $a(X)$ and $b(X)$: there exist polynomials $m(X)$ and $n(X)$ such that

$$\gcd\big(a(X), b(X)\big) = m(X)a(X) + n(X)b(X). \tag{2.5}$$

2.4 Prime Factorization

Let us say that a polynomial $p(X)$ is *prime* if it is not constant and its only divisors are $p(X)$ and 1 (and constant multiples of them).

For $\mathbf{Z}[X]$, we need to be careful: $p(X)$ is prime inside $\mathbf{Z}[X]$ if it is not equal to ± 1 and its only divisors in $\mathbf{Z}[X]$ are $\pm p(X)$ and ± 1.

Thus, the constant 3, thought of as a polynomial is prime in $\mathbf{Z}[X]$, but the constant 4 is not prime in $\mathbf{Z}[X]$. Neither is prime in $\mathbf{Q}[X]$.

A polynomial of degree ≥ 1 which cannot be factored into polynomials of degree ≥ 1 is called *irreducible*.

Thus, a first degree polynomial

$$3X-4$$

is irreducible.

The polynomial

$$X^2-4$$

is not irreducible because

$$X^2-4=(X-2)(X+2).$$

But how about X^2-2? If we stick to rational numbers as coefficients, then it is irreducible. But if we allow irrational numbers (or at least $\sqrt{2}$ and all related numbers) then X^2-2 is reducible:

$$X^2-2=(X-\sqrt{2})(X+\sqrt{2}).$$

Similarly,

$$X^2+1$$

is irreducible over reals but reducible when $i=\sqrt{-1}$ is included in the field of allowed coefficients.

Exactly as with numbers, we have the following results:

(i) If $a(X)$, $b(X)$, and $c(X)$ are polynomials such that $a(X)$ is a divisor of $b(X)c(X)$,and $a(X)$ is co-prime to $b(X)$, then $a(X)$ is a divisor of $c(X)$. Compare with Proposition 1.

(ii) Every polynomial is the product of prime polynomials in a unique way (uniqueness only up to constant multiples). This is true also in $\mathbf{Z}[X]$, with uniqueness up to multiplication by ± 1.

2.5 Descartes' Theorem on Factors of Polynomials

There is another remarkable dividend we can draw from our efforts in proving the division algorithm for polynomials. This is Descarte's theorem on roots of polynomial equations:

Theorem 5 *Let $p(X)$ be a polynomial of degree ≥ 1. Then the equation*

$$p(x) = 0$$

has a solution $x = \alpha$ if and only if $X - \alpha$ is a divisor of $p(X)$.

To prove this, consider the division of $p(X)$ by $X - \alpha$:

$$p(X) = q(X)(X - \alpha) + r,$$

and the remainder r mult be a constant, because it has lower degree than $X - \alpha$. Now substitute in the value α for X to get:

$$p(\alpha) = 0 + r.$$

Thus, *the remainder r is actually the value of $p(x)$ when x is set equal* α. In particular,

$p(\alpha)$ is 0 if and only if the remainder r is 0,

which is the same as saying that $p(X)$ is divisible by $X - \alpha$. This proves Descartes' theorem.

René Descartes was on born March 31, 1596 in France. He is best known for his contributions to mathematics and philosophy. He died on February 11, 1650, in Sweden, of pneuomonia while working as tutor to the queen of Sweden (other theories, involving arsenic poisoning have been proposed).

From Descartes' theorem we see that an n-th degree polynomial equation can have at most n roots, for the product of more than n terms like $X - \alpha$ would have degree more than n.

Moreover, we also see that if $p(X)$ factorizes completely as

$$p(X) = a(X - \alpha_1)...(X - \alpha_n),$$

where a is a non-zero constant, then the roots of

$$p(x) = 0$$

are $\alpha_1, ..., \alpha_n$.

2.6 Newton Polynomials

Consider the product:

$$(X-\alpha_1)(X-\alpha_2) = X^2 - \alpha_1 X - \alpha_2 X + \alpha_1\alpha_2,$$

which we can write as

$$(X-\alpha_1)(X-\alpha_2) = X^2 - (\alpha_1+\alpha_2)X + \alpha_1\alpha_2.$$

Next, we have

$$(X-\alpha_1)(X-\alpha_2)(X-\alpha_3) = X^3 - (\alpha_1+\alpha_2+\alpha_3)X^2 + (\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3)X - \alpha_1\alpha_2\alpha_3.$$

Continuing in the vein, consider the product:

$$(X-\alpha_1)...(X-\alpha_n).$$

This works out to

$$X^n - (\alpha_1+\cdots+\alpha_n)X^{n-1} + (\alpha_1\alpha_2+\cdots)X^{n-2} + \cdots + (-1)^n\alpha_1...\alpha_n.$$

The coefficient of X^{n-k} is $(-1)^k$ times the sum of all products of k of the quantities $\alpha_1,...,\alpha_n$.

In view of this, it makes sense to introduce the following polynomials in n variables $T_1,...,T_n$:

$$s_1(T_1,...,T_n) = T_1 + \cdots + T_n$$

$$s_2(T_1,...,T_n) = T_1T_2 + T_1T_3 + \cdots + T_1T_N + \cdots + T_{n-1}T_n,$$

and so on till

$$s_n(T_1,...,T_n) = T_1...T_n.$$

More precisely,

$$s_k(T_1,...,T_n) = \sum_{1\le j_1<\cdots<j_k\le n} T_{j_1}...T_{j_k}. \tag{2.6}$$

These polynomials are called *Newton polynomials* (Isaac Newton ((4 January 1643 – 31 March 1727). The first thing to note about them is that they are *symmetric in the variables $T_1,...,T_n$*.

Secondly, we note that

$$(X-\alpha_1)...(X-\alpha_n) = X^n - s_1(\alpha_1,...,\alpha_n)X^{n-1} + \cdots + (-1)^n s_n(\alpha_1,...,\alpha_n). \tag{2.7}$$

To take a specific example, consider the equation

$$x^3 - 4x^2 - 5x - 2 = 0.$$

Let α, β, γ be the roots of the equation. Then the Newton polynomials in these roots have the values

$$s_1(\alpha,\beta,\gamma) = 4, \quad s_2(\alpha,\beta,\gamma) = -5, \quad s_3(\alpha,\beta,\gamma) = -2.$$

Note that for an equation such as

$$5x^4 - 2x^3 + 6x + 8 = 0,$$

we have to be careful about that coefficient 5and note that if the roots are $\alpha, \beta, ...$ then

$$\begin{aligned} 5X^4 - 2X^3 + 6X + 8 &= 5(X-\alpha)(X-\beta)....\\ &= 5(X^5 - s_1X^4 + s_2X^3 - \cdots). \end{aligned} \tag{2.8}$$

Consequently, here

$$s_1(\alpha,...) = \frac{2}{5},...$$

and so on, till s_5 which is equal to $-8/5$.

In class we proved the following remarkable result:

Theorem 6 *Every symmetric polynomial $p(T_1,...,T_n)$ can be expressed as a polynomial in the Newton polynomials.*

For example, for two variables T_1 and T_2: we have

$$T_1^2 + T_2^2 = (T_1 + T_2)^2 - 2T_1T_2 = s_2^2 - 2s_2.$$

2.7 The Discriminant

Now consider a quadratic (with 1 as leading coefficient):

$$p(X) = X^2 - s_1X + s_2 = (X-\alpha)(X-\beta).$$

Let

$$\Delta = \alpha - \beta.$$

The quantity

$$\Delta^2 = (\alpha - \beta)^2$$

is called the *discrimininant* of $p(X)$. The point is that, the discriminant is 0 if and only if the two roots of $p(x) = 0$ are equal.

Note that

$$\Delta = \alpha - \beta$$

flips to its negative if α and β are interchanged. So the square, Δ^2 is *symmetric* in α and β. Being a symmetric polynomial it can be rewritten in terms of Newton's polynomials. Indeed,

$$(\alpha - \beta)^2 = \alpha^2 - 2\alpha\beta + \beta^2 = (\alpha + \beta)^2 - 4\alpha\beta.$$

Thus, the discriminant is

$$\Delta^2 = s_2^2 - 4s_2.$$

In more familiar language, the discriminant of

$$x^2 + Bx + C$$

is

$$B^2 - 4C.$$

If the leading coefficient is not 1, we define the discriminant of

$$A(X - \alpha)(X - \beta)$$

to be

$$\Delta^2 = A^2(\alpha - \beta)^2. \tag{2.9}$$

Then for the quadratic

$$AX^2 + BX + C = A(X - \alpha)(X - \beta) = AX^2 - As_1X + As_2,$$

the discriminant works out to

$$A^2(\alpha - \beta)^2 = A^2\left(\left(\frac{B}{A}\right)^2 - 4\frac{C}{A}\right) = B^2 - 4AC,$$

the usual expression for the discriminant.

Now consider the cubic

$$AX^3 + BX^2 + CX + D = A(X - \alpha)(X - \beta)(X - \gamma).$$

The discriminant is defined to be the square of

$$\Delta = A(\alpha - \beta)(\alpha - \gamma)(\beta - \gamma).$$

This Δ is again *anti-symmetric* with repect to interchange of roots, and so the discriminant is again a *symmetric polynomial* α, β, γ. Consequently, Δ^2 can be expressed in terms of the Newton polynomials in α, β, γ, and hence in terms of the coefficients $A, ..., D$.

Thus, it possible to construct a polynomial in the coefficients $A, ..., D$ such that this vanishes if and only if the original cubic has two equal roots.

2.8 The Derivative

Introduce a new quantity ε with the property that

$$\varepsilon^2 = 0.$$

Let us work out some calculations with this, for polynomials.

First we have

$$(X + \varepsilon)^2 = X^2 + 2\varepsilon X + \varepsilon^2 = X^2 + 2\varepsilon X.$$

Similarly,

$$(X + \varepsilon)^3 = X^3 + 3X^2\varepsilon.$$

More generally,

$$(X + \varepsilon)^n = X^n + nX^{n-1}\varepsilon.$$

For a polynomial

$$p(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0,$$

we then have

$$p(X + \varepsilon) = p(X) + p'(X)\varepsilon,$$

where $p'(X)$ is the *derivative* of $p(X)$ defined to be

$$p'(X) = a_n n X^{n-1} + a_{n-1}(n-1)X^{n-2} + \cdots + a_1.$$

We also write

$$Dp(X)$$

for $p'(X)$.

Consider now the effect of changing X to $X+\varepsilon$ in the product of two polynomials $p(X)$ and $q(X)$:

$$\begin{aligned} p(X+\varepsilon)q(X+\varepsilon) &= \big(p(X)+p'(X)\varepsilon\big)\big(q(X)+q'(X)\varepsilon\big) \\ &= p(X)q(X)+[p'(X)q(X)+p(X)q'(X)]\varepsilon+0. \end{aligned} \tag{2.10}$$

This proves that

$$D[p(X)q(X)] = p'(X)q(X)+p(X)q'(X) \tag{2.11}$$

We have also seen in class that the chain rule holds:

$$D[p(q(X))] = p'(q(X))q'(X). \tag{2.12}$$

2.9 Multiple Roots and the Derivative

Consider the equation

$$2x^3-3x^2+1=0. \tag{2.13}$$

As it happens,

$$2X^3-3X^2+1=(X-1)^2(2X+1),$$

and so the equation (2.13) has roots $1,1,-1/2$. The root 1 is repeated.

We will now determine a way to figure out that (2.13) has a repeated root, without having to solve the equation. The method will work even for equations such as

$$x^{15}-7x^8+3x-4=0,$$

which cannot be solved exactly by the usual methods.

Let us write

$$a(X)=2X^3-3X^2+1$$

and suppose α,β,γ are the roots of (2.13). Then, by Decarte's theorem, $a(X)$ factorizes as

$$a(X)=2(X-\alpha)(X-\beta)(X-\gamma).$$

Let us now look at the derivative

$$a'(X).$$

This works out to be

$$a'(X) = 2[(X-\beta)(X-\gamma)+(X-\alpha)(X-\gamma)+(X-\alpha)(X-\beta)].$$

Observe that

$$a'(\alpha) = 2(\alpha-\beta)(\alpha-\gamma).$$

Also,

$$a'(\beta) = 2(\beta-\alpha)(\beta-\gamma),$$

and

$$a'(\gamma) = 2(\gamma-\alpha)(\gamma-\beta).$$

To have a repeated root means that at least one pair of the roots α, β, γ are equal to each other. But then, looking at the preceding expressions, that this is precisely the condition that one of the values $a'(\alpha)$, $a'(\beta)$, $a'(\gamma)$ is 0.

Thus, *the equation (2.13) has a repeated root if and only if that root is also a root of the equation*

$$a'(x) = 0.$$

Looking back at the expression for $a(X)$, we have

$$a'(X) = 6X^2 - 6X = 6X(X-1).$$

The roots of $a'(x) = 0$ are therefore $x = 0$ and $x = 1$. We can substitute 1 for X in $a(X)$ and find that

$$a(1) = 2-3+1 = 0,$$

and so indeed the equations $a(x) = 0$ and $a'(x) = 0$ share a common root 1. Therefore, we can tell right away that this root must be a repeated root of $a(x) = 0$.

Before moving on to the general statement, let us note that to say that $a(x) = 0$ and $a'(x) = 0$ have a common root is equivalent to saying that there is some α such that $X - \alpha$ is a divisor of both $a(X)$ and $a'(X)$. Thus, the condition of repeated roots is that $a(X)$ and $a'(X)$ should have a common divisor of degree ≥ 1.

Everything we have done can be easily checked to hold for a general polynomial $p(X)$ of degree ≥ 1. Thus, we have

Theorem 7 *If $p(X)$ is a polynomial of degree ≥ 1 then the equation*

$$p(x) = 0$$

has repeated roots if and only if $\gcd(p(X), p'(X))$ *has degree* ≥ 1.

Let us do a simple example. Consider the equation

$$x^2 + x + 1 = 0.$$

Does it have repeated roots? The derivative of

$$p(X) = X^2 + X + 1$$

is

$$p'(X) = 2X + 1.$$

The gcd works out to

$$\gcd\big(p(X), p'(X)\big) = 1.$$

(Note that the gcd is specified only up to constant multiples, and we could write any non-zero constant in place of 1.) Thus,

$$x^2 + x + 1 = 0$$

has no repeated roots.

In this particular example, we could have easily solved the equation to see that the roots are indeed different. We could also have seen that the solution of $p'(x) = 0$ is $x = -1/2$ and this is not a solution of $p(x) = 0$.

Problem Sets 3 and 4

Problems 1-3 below are adapted, with some simplification, from Euler's 'Elements of Algebra' (first published 1770).

1. Show that

   $$\left(\frac{3}{2} + \frac{1}{2}\sqrt{21}\right)^3$$

   is $27 + 6\sqrt{2}$.

2. Carry out a transformation which turns the equation

   $$x^3 - 6x^2 + 13x - 12 = 0$$

   into a cubic equation of the form

   $$y^3 + y - 2 = 0$$

3. Use the Cardano method to find one solution of the equation

$$y^3 = (-1)y + 2.$$

Bring the solution to the form

$$\left[1+\frac{6}{27}\sqrt{21}\right]^{1/3} + \left[1-\frac{6}{27}\sqrt{21}\right]^{1/3}.$$

Use Problem 1 to simplify this expression to show that this gives the solution $y = 1$.

4. Find all three solutions of the equation

$$x^3 - 6x^2 + 13x - 12 = 0$$

5. Find a solution of

$$x^4 - 10x^3 + 35x^2 - 50x + 24 = 0 \tag{2.14}$$

by using Ferrari's method as follows. The goal will be to find values for p, q, and r such that

$$x^4 - 10x^3 + 35x^2 - 50x + 24 = (x^2 - 5x + p)^2 - (qx + r)^2. \tag{2.15}$$

(i) Show that we should chooose p, q, and r to satisfy

$$\begin{aligned} q^2 &= 2(p-5) \\ r^2 &= p^2 - 24 \\ qr &= 5(p-5). \end{aligned} \tag{2.16}$$

(ii) Work out q^2r^2 and $(qr)^2$ from the equations in (i), and show that p satisfies the cubic equation

$$2(p-5)(p^2-24) - 25(p-5)^2 = 0.$$

(iii) Take the solution $p = 5$ and work out corresponding values of q and r from part (i).

(iv) Now substitute the values of p, q, and r, into equation (2.15), and find all solutions of the original quartic equation

$$x^4 - 10x^3 + 35x^2 - 50x + 24 = 0.$$

6a. Suppose the polynomial $p(X) = 3X^3 - 2X^2 + 4$ factors as

$$3X^3 - 2X^2 + 4 = 3(X - \alpha)(X - \beta)(X - \gamma)$$

(i) The value of $\alpha + \beta + \gamma$ is:

(ii) The value of $\alpha\beta\gamma$ is:

(iii) The value of the Newton polynomial s_2 is:

(iv) The derivative $p'(X)$ is:

(v) If $\alpha = \beta$ what is the value of $p'(\alpha)$?

6b. Suppose the polynomial $p(X) = 7X^5 - 5X^3 + 3$ factors as

$$7X^5 - 5X^3 + 3 = 7(X - \alpha_1)(X - \alpha_2)\dots(X - \alpha_7)$$

(i) The value of $\alpha_1 + \cdots + \alpha_7$ is:

(ii) The value of $\alpha_1 ... \alpha_7$ is:

(iii) The value of the Newton polynomial s_4 is:

(iv) The derivative $p'(X)$ is:

(v) If $\alpha_1 = \alpha_3$ what is the value of $p'(\alpha_3)$?

7. Work out the quotient and remainder for the following divisions:

(i) Divide $X^2 - 3X + 3$ by $X - 1$.

(ii) Divide $X^3 - 2$ by $X + 1$.

(iii) Divide $X^3 - 2$ by $X^2 - X + 1$.

8. Work out the greatest common divisors for:

(i) $X^2 - 3X + 3$ and $X - 1$.

(ii) $X^2 - 3X + 2$ and $X^3 - 3X^2 + 3X - 1$.

(iii) $X^{12} - 2$ and X^{11}.

9. Work out the derivatives of:

(i) $X^2 - 3X + 3$.

(ii) $X^3 - 3X^2 + 3X - 1$.

(iii) $X^{12} - 2$.

(iv) $X^3 + X^2 + X + 1$.

(v) $4(X-3)(X-2)(X+7)$.

(vi) $-3(X-2)(X-2)(X-3)$.

10. Determine which of the following equations have repeated roots:

(i) $x^2 - 6x + 3 = 0$.

(ii) $x^3 + x^2 - x - 1 = 0$.

(iii) $x^2 + x + 1 = 0$.

(iv) $x^5 - 1 = 0$.

(v) $x^{15} - 1 = 0$.

Chapter 3

Geometry

In this chapter, we shall take a quick look at the axiomatic construction of geometry. Our objective is not so much a study of the axioms, as an appreciation of how they lead to number systems, and, in particular, the real number system. Euclid's geometric constructions, such as those involving similar triangles, implicitly *describe a process of addition and, more importantly, multiplication of ratios of segments*. Euclid's results imply then that these operations satisfy the usual algebraic laws: commutativity, associativity, and distributivity of multiplication over addition. If one agrees to adjoin to this system, the number 0 and 'negatives' (which, of course, came much later in history) of all the segment ratios, then one obtains a *field*. If one uses a sufficiently strong axiom of 'completeness', this yields the entire real number system. Even without this strong completeness axiom, Euclid's constructions lead to what are now called extensions of the field of rationals.

A thorough and logical study of geometry was carried out by Greek mathematicians. Some books from this era have survived, at least in fragmentary form, often through later Arabic translations. The most famous of these works is Euclid's *Elements*. Great mathematical figures from this era include (the dates are approximate):

- Thales of Miletus (624 BC-546 BC)
- Pythagoras (580 BC–500 BC)
- Eudoxus (410BC - 3550 BC)
- Euclid (325 BC–265 BC)
- Archimedes (287 BC - 212 BC)

- Apollonius (262 BC–190 BC)

The geometric ideas of Thales and Pythagoras seem to have been influenced by Egyptian mathematics. In the context of geometry, Eudoxus is best known for his theory of proportions and the method of exhaustion, which are early precursors of the modern theory of real numbers and integral calculus. Apollonius is best known for his work on conic sections, possibly the deepest part of Greek mathematics.

Euclid's development of geometry included:

- Definitions
- Axioms
- Theorems
- Geometric Constructions.

The topic of geometric constructions, using ruler and compass, is connected, in a thread developed far later in history, to algebra and solutions of algebraic equations.

Euclid's axiomatic treatment of geometry did have some unrecognized assumptions. A complete logical development of geometry was provided by Hilbert (1862-1943) in his book *Grundlagen der Geometrie* [1], first in 1899 and then with many refinements and developments in succeding editions of the book.

3.1 Hilbert's Axioms for Plane Geometry

Hilbert laid out the axiomatic development of three-dimensional Euclidean geometry. Here we shall focus on two-dimensional geometry, drawing the axioms from Hilbert [1].

There are two basic objects in plane geometry: *points* and *lines*.

Let $\mathcal{P}$ denote the set of all points, and $\mathcal{L}$ the set of all lines.

3.1.1 Axioms I: Incidence

The notion of a 'point lying on a line' is codified through a set I consisting of ordered pairs (p,l), where p is a point and l a line. Thus, I is a subset of $\mathcal{P}\times\mathcal{L}$. If $(p,l)\in I$ we say that 'point p lies on the line l.' We also say in this case that the line l 'passes through' the point p. This relation is called the *incidence relation*.

The following are the axioms of incidence for plane geometry:

I1. For any two distinct points, there is one and only one line that passes through both of them.

I2. On any line, there exist at least two distinct points.

I3. There exist three points which are non-collinear, i.e. there is no line passing through all of them.

Axiom I1 (which is split into two in Hilbert's book) appears in a manner in Book I of Euclid, and the others are taken for granted.

If two distinct lines both pass through a common point then we say that the lines *cross* at this point. Because of I1, it follows that two distinct lines can have at most one point of crossing.

Lines l and m are said to be *parallel* if either $l = m$ or if l and m do not cross.

A set of points and lines, along with a collection I, is said to form an *incidence geometry*, if Axioms I1, I2,I3 hold. Because of I3, any incidence geometry must contains at least 3 points.

Thus, the simplest example of incidence geometry is given by $\mathcal{P} = \{A,B,C\}$, with three lines, each specified uniquely by a pair of distinct points. Thus, we can denote the lines by $\{A,B\}$, $\{A,C\}$, and $\{B,C\}$. The incidence relation is specified in the obvious way: for example, point B lies on lines $\{A,B\}$ and $\{B,C\}$.

Next, consider as $\mathcal{P}$ a set with four distinct elements A,B,C,D. Take as lines all pairs of distinct points: $\{A,B\}$, $\{A,C\},\{A,D\},\{B,C\},\{B,D\},\{C,D\}$. This gives the four-point incidence geometry.

3.1.2 Axioms II: Order

The next concept systematized by Hilbert is that of 'betweenness' or order. This concept was implicit in Euclid's Elements, and the axioms were used without being recognized.

Betweenness is specified by a set $\mathcal{B}$ of ordered triples of points. If $(A,B,C) \in \mathcal{B}$ we read this as *point B lies between points A and C*.

The axioms for $\mathcal{B}$ are:

B1. If $(A,B,C) \in \mathcal{B}$ then A, B, and C are three distinct collinear points, i.e. they all lie on one common line.

B2. If $(A,B,C) \in \mathcal{B}$ then $(C,B,A) \in \mathcal{B}$, i.e. if B lies between A and C then B lies between C and A.

B3. If A and B are two distinct points on a line then there is a point C on this line such that B lies between A and C.

B4. For any three distinct points on a line, at most one of them lies between the other two. (See Theorem 9 below.)

B5. If A, B, C are three non-collinear points, and l a line not through any of them, and if l passes through a point between A and C, then l passes through a point between A and B or through a point between B and C.

The Axiom B5 is best understood by drawing a diagram of a triangle ABC and a line cutting through the side AB. It should be clear that B5 works only on a plane, so that a line has no way of 'escaping' off the triangle once it has crossed into it through one side. This axiom was used in Euclid's *Elements* without being recognized as an assumption.

In the context of B5, it can be proved that the line l cannot pass through points between A and B, between B and C, and between C and A.

Axiom B5 allows us to construct points between two points. This is formalized in:

Theorem 8 *Between any two distinct points lies at least one point.*

Proof. First note that Axiom B5 provides the *existence* of a point in this context, and so we should try to use this axiom. Thus, we should construct a triangle ABC and a line which, by construction, passes through, say, a point between A and C; this would imply that it passes through a point between A and B.

Let A and B be distinct points. By I3, there is a point D not on the line through A and B. By B3, there is a point C such that D lies between A and C. Again, by B3, there exists a point E such that B lies between C and E. Consider the line l through D and E. This line passes through the point D. By B5, l passes through a point between A and B or a point between A and C. But the latter possibility would again imply that A, B, C all lie on l. Thus, l passes through a point between A and B, and so there is a point between A and B. $\boxed{\text{QED}}$

Consequently, there are infinitely many points between any two distinct points.

In the first edition of Hilbert's book the following result (proved later by E. H. Moore) was taken as an axiom:

Theorem 9 *For any three distinct points on a line, at least one of them lies between the other two.*

The following results says that a line partitions of all the points outside it into two disjoint classes, called the two *sides* of the line:

Theorem 10 *If l is a line then the set of all points not on l is the union of two non-empty disjoint subsets, such that two points not on l lie in the same subset if and only if l does not pass through a point between them.*

A similar result holds for lines:

Theorem 11 *If l is a line, and O a point on it, then the set of all points on l other than O are partitioned into two disjoint subsets: two points of l other than O lie in the same subset if and only if O does not lie between them.*

3.1.3 Some Definitions: Segment, Ray, and Angle

The definitions here differ slightly from Hilbert's. For example, we view the endpoints as being points on a segment, and we view the vertex of a ray as being part of the ray.

If A and B are distinct points then the *segment* $\overline{AB}$ is the set consisting of points A and B along with all points between A and B.

Consider a point O on a line l. The points on l, other than O, are partitioned into two disjoint classes by O: for points X and Y on l other than O, we say that X and Y are *on opposite sides* of O if O lies between them; we say that they are on the *same side* of O if O does not lie between them.

Points A and B, not on a line l, lie on *opposite sides* of a line l if l contains a point between A and B; otherwise, we say that A and B lie on the *same side* of l.

If A is a point on a line l then, for any other point B on l, the *ray* $\vec{AB}$ consists of all points C on l on the same side of A as B, along with A itself. The *vertex* A of the ray is identified as the unique point in the ray which does not lie between two points on the ray.

Two rays are said to be *opposite* if they are of the form $\vec{AB}$ and $\vec{AD}$, where D, A and B are collinear, with A between D and B.

An *angle* with vertex X is a pair of distinct rays $\vec{XY}$ and $\vec{XZ}$ which are not on a common line. (It is convenient, for the sake of a clean formulation of the axioms, to exclude the 'straight angles'.) This angle is denoted

$$\langle ZXY.$$

By definition, the order of the rays $\vec{XY}$ and $\vec{XZ}$ does not matter, and so

$$\langle ZXY = \langle YXZ.$$

A point P lies in the *interior* of the angle $\langle XYZ$ if P does not lie on the rays $\vec{YZ}$ and $\vec{YX}$ and if P lies on the same side of the line YZ as X and on the same side of line YX as Z. This is best understood through a picture.

We define a *triangle* to be a set of three non-collinear points called the *vertices* of the triangle. A segment specified by any pair of the vertices is called a *side* of the triangle.

3.1.4 Axioms III: Congruence

Next are introduced two relations of *congruence*.

Congruence of segments is given by a set $\mathcal{C}$ of ordered pairs of segments. If $(x,y) \in \mathcal{C}$ we say that segment x is congruent to segment y. We denote this by

$$x \equiv y$$

CS1. If A and B are two points, and A' a point, then on any ray with vertex A' lies a point B' such that $\overline{AB}$ is congruent to $\overline{A'B'}$.

CS2. If segment $\overline{AB}$ and segment $\overline{CD}$ are congruent to the same segment then $\overline{AB}$ is congruent to $\overline{CD}$.

CS3. If $\overline{AB}$ and $\overline{BC}$ are two segments on a line, with B the only point in common, and if $\overline{A'B'}$ and $\overline{B'C'}$ be two segments on a line with B' the only point in common, and if, further, $\overline{AB}$ is congruent to $\overline{A'B'}$ and if $\overline{BC}$ is congruent to $\overline{B'C'}$ then $\overline{AC}$ is congruent to $\overline{A'C'}$.

Sometimes we will write just AB to mean the segment $\overline{AB}$.

We can now check that congruence is an equivalence relation:

- Reflexivity: If AB is a segment, and A' any point then, by CS1, there is a segment $A'B'$ to which AB is congruent. Thus, trivially, AB and AB are both congruent to $A'B'$, and so AB is congruent to itself.

- Symmetry: Next, if AB is congruent to CD then, since CD is also congruent to CD, we see that both CD and AB are congruent to CD; then it follows by CS2 that CD is congruent to AB.

- Transitivity: Finally, suppose segment x is congruent to segment y, and y is congruent to z; then, x and z are both congruent to y, and so x is congruent to z.

The significance of axiom CS3 is that it allows us to *add* segments by placing them 'next to each other.'

Let us recall that a ray h is a set consisting of a point O, called the vertex of h, another point B, and all points on the line through O and B which are on the same side of O as B. In this case we denote h by $\vec{O}B$. An angle is a pair $\{h,k\}$ of non-collinear rays with a common vertex. We denote this angle by

$$\langle(h,k).$$

If $h=\vec{O}A$ and $k=\vec{O}B$ we write this same angle as

$$\langle AOB,$$

or, when the rays $\vec{O}A$ and $\vec{O}B$ are understood from context, even as simply

$$\langle O.$$

There is also a second notion of congruence which applies to angles, and we use the same notation $\equiv$ for angle congruence. The axioms for congruence of angles are:

CA1. Given any angle x and a ray $\vec{X}Y$ and a point P not on the line l through X and Y, there is a unique ray $\vec{X}Z$ such that Z lies on the same side of l as P and the angle $\langle ZXY$ is congruent to x.

CA2. Every angle is congruent to itself.

CA3. If ABC and $A'B'C'$ are triangles such that segment AB is congruent segment $A'B'$, and segment AC is congruent to segment $A'C'$, and also $\langle BAC$ is congruent to $\langle B'A'C'$, then $\langle ABC$ is congruent to $\langle A'B'C'$.

A triangle T is said to be *congruent* to a triangle T' if the vertices of T can be labeled ABC and the vertices of T' as $A'B'C'$ in such a way that

$$\overline{AB}\equiv\overline{A'B'},\ \overline{BC}\equiv\overline{B'C'},\ \overline{CA}\equiv\overline{C'A'}$$

and

$$\langle A\equiv\langle A',\ \langle B\equiv\langle B',\ \langle C\equiv\langle C'$$

The axioms imply all the Euclidean results on congruence of triangles, and, furthermore, also imply that congruence for angles as well as for triangles are equivalence relations.

Two angles x and y are said to be supplementary if there is a point B between two points A and C, and a point D outside the line through A and C, such that $x \equiv \langle DAC$ and $y \equiv \langle DAB$.

It may be proved that each angle has a unique supplementary angle, up to congruence.

A *right angle* is an angle which is congruent to its supplementary angle.

3.1.5 Axiom of Parallelism

Lines l and l' are *parallel* if either $l = l'$ or if l and l' have no point in common. We also say that 'l is parallel to l''.

Hilbert's axiom of parallelism is:

HP. If l is a line and P a point not on it, then through P there is at most one line parallel to l.

In contrast to this, Euclid's axiom on parallelism states that through any point outside a line l there *exists* a unique line parallel to l. Hilbert does not need to assume the existence of a parallel line, because the existence of such a line can be *proved* from the other axioms.

We can now state and prove our first theorem of geometry:

Theorem 12 *If lines l and m are parallel, and lines m and n are parallel, then l and n are parallel.*

Proof. If, to the contrary, l and n were distinct and a point P were common to them, then through P there would be two distinct lines, l and n, both parallel to m. This is impossible by the Hilbert parallel axiom, and so l and n are parallel. $\boxed{\text{QED}}$

Using HP, it can be proved that the three angles of a triangle 'add up to 180 degrees'; more precisely, if ABC is a triangle, and O any point lying between two points P and Q then there exists a point S outside the line PQ and a point T in the interior of $\langle QOS$, such that

$$\langle SOP \equiv \langle A, \langle TOS \equiv \langle B, \langle QOT \equiv \langle C.$$

3.1.6 Axiom of Continuity or Completeness

A classical axiom fundamental to the real number system is:

AC. *Axiom of Archimedes*: If A, B, C are distinct points, then there is a positive integer $n \in \{1,2,3,...\}$, such that n times the segment AB exceeds the segment AC. In more detail, there are points $P_1,...,P_n$ on the ray $\vec{AC}$, such that :(i) P_1 lies between A and P_2; (ii) for each $k \in \{2,...,n-1\}$, the point P_k lies between P_{k-1} and P_{k+1}; (iii) each segment $\overline{P_kP_{k+1}}$ and the segment $\overline{AP_1}$ is congruent to $\overline{AB}$; and (iv) the point C lies between A and P_n.

The preceding system of axioms do not uniquely specify the geometry, in the sense that there are non-isomorphic systems of points and lines which satisy all the preceding axioms. There is, of course, nothing wrong with having a system of axioms covering a large array of examples.

Hilbert introduces a final axiom of maximality:

M. The set of points on a line cannot be enlarged in such a way that the larger set of points also have an ordering and congruence for which all the axioms mentioned above hold.

Of course, in principle this axiom could be inconsistent with the previous axioms. However, that is not the case. Indeed, the maximal geometry exists and satisfies the Dedekind completeness property:

D. If the points of a line l are partitioned into two non-empty disjoint sets S and S' in such a way that no point of one set is between two points of the other set then there exists a unique point P on l which lies between any point of S (other than P) and any point of S' (other than P).

3.2 Constructions with Ruler and Compass

An important enterprise within Euclidean geometry was the construction of geometrical figures using two devices: a straight edge (ruler) and a compass. The ruler was used to draw straight lines and the compass to draw circles with given center and radius.

The axioms of congruence of segments and angles include the fact that segments and angles can be *transported*:

CS1. If A and B are two points, and A' a point, then on any ray with vertex A' lies a point B' such that $\overline{AB}$ is congruent to $\overline{A'B'}$.

CA1. Given any angle x and a ray $\vec{XY}$ and a point P not on the line l through X and Y, there is a unique ray $\vec{XZ}$ such that Z lies on the same side of l as P and the angle $\langle ZXY$ is congruent to x.

The traditional Paltonic instruments of ruler and compasses are vehicles for transporting segments and angles to congruent copies. Thus, ruler and compass constructions are not simply some odd historical curiosity involving primitive devices available at some period in history, but rather essential to the axiomatic framework of geometry. The constructions of Euclid, starting from a given set of points, produce lines and points which satisfy the axioms of geometry (except for the Dedekind axiom) and thus, as we shall see later, produce an algebraic system called a *field*.

A *circle* with center C and radius specified by a segment $\overline{OR}$ is the set of all points P such that the segment $\overline{CP}$ is congruent to the given segment $\overline{OR}$. If two distinct points A and B lie on a circle with center C and if A, B, and C are collinear then we say that the segment $\overline{AB}$ is a *diameter* of the circle, and the points A and B are said to be diametrically opposite to each other.

An *arc* of a circle requires some more effort to define. Consider a circle with center C, and suppose that P and Q are two distinct points on the circle which don't form a diameter. Then the *arc* $\hat{PQ}$ is the set of all points X on the circle such that X lies on the same side of CQ as P and also on the same side of CP as Q.

Consider a set S of points.

Let us say that a line is *directly constructible* from S if it passes through two points of S. We think of this as a line drawn by placing a ruler against the two points of S.

Let us also say that a circle is *directly constructible* from S if it has center at a point of S and has radius given by a segment $\overline{OR}$ for some points O and R of S.

Thus, starting with a set of points we have constructed, in one step, a set of lines and circles. Now we can look at the set of all points where these lines and circles intersect.

We shall say that a point is directly constructibe from a given set of lines and circles if it lies on at least two of these figures (lines or circles). Such a point can lie on two lines, two circles, or a line and a circle.

Thus, starting with a set of points we can carry out constructions as above, obtaining sets of lines and circles, from which we generate another set of points, which can again be used to generate more lines and circles.

Any line or circle or segment or point which can be obtained by a finite sequence of constructions as above can thus be said to be *constructible* with ruler and compasses from the initial given set S of points.

It is very important to realize that not all points on a constructible line are constructible. *Only points where constructible lines or circles cross are constructible.*

By a geometrical figure let us mean a finite set of points, lines, circles, segments, and arcs. For example, a pentagon is a geometrical figure. Euclid described numerous constructions of geometrical figures.

There were three famous construction problems from the Greek era which were not solved:

- Squaring the circle: constructing a square the same area as a given circle.
- Doubling the cube: constructing a cube with twice the volume of a given cube.
- Trisecting the angle: dividing a given angle into three smaller angles all congurent to each other.

The first two involve measures of area and volume which we have not examined in these notes.

In 1796 Gauss (Carl Friedrich Gauss, 1777 –1855) constructed a regular 17-gon and determined a criterion for constructibility of a regular n-gon based on the prime factors of n. That Gauss's method determined all constructible regular polyons was proved by Wantzel in 1837. You can find Gauss's construction online (for example, at http://www.answers.com/topic/heptadecagon).

3.3 Theory of Proportions

A theory of proportions was developed by Eudoxus and appears in Euclid's *Elements*. Proportions of 'like magnitudes' are considered; for example, proportions between segments, or areas and volumes were considered. In our discussion here we will focus on segments.

In this section we will denote a segment without the bar on top, i.e. as AB instead of $\overline{AB}$.

It will sometimes be convenient to identify congruent segments. The set of all segments congruent to AB will be denoted [AB]. Let S be the set of all such segment classes [AB].

It makes sense to add segments: just lay them side by side. By the congruence axiom CS4, this addition is a meaningful operation on S. If $x, y \in S$ we can 'add' them to produce an element $x + y$.

It may be checked that this addition has the basic nice properties:

$$x + y = y + x, \qquad \text{and} \qquad x + (y + z) = (x + y) + z.$$

However, there is no natural way to 'multiply' two segments to produce another segment. One insight behind the theory of proportions is that it creates in a natural way, a system of quantities - *ratios* between segments - for which there is both a meaningful addition operation and a multiplication operation. It will take some work to see how this emerges.

If m is a positive integer $\in \{1, 2, 3, ...\}$ we shall denote by mAB the segment running from A to a point P such that between A and P there are points which mark off m congruent segments (if $m = 1$ then we just have 1.AB=AB, by definition). On the set S we have a corresponding operation, producing positive integer multiples $2x, 3x, ...$ of any $x \in S$.

Let us agree to say that segment AB is *greater* than a segment PQ, if there is a point C between A and B such that AC is congruent to PQ. In this case we shall write

$$AB > PQ,$$

or

$$PQ < AB.$$

You can check that if AB>PQ then PQ is not greater than AB. Moreover,

if AB>CD and CD>EF then AB>EF.

Thus, we have an order relation $x > y$ between elements $x, y \in S$.

If AB and CD are segments there is associated to this pair the proportion

$$AB : CD.$$

We can think of this simply as a new object, an ordered pair of segments.

In *Elements* Volume 5, Euclid defines when a ratio is equal to another. If AB, CD, PQ, RS are segments we declare

$$AB : CD \simeq PQ : RS$$

if a multiple of AB exceeds a multiple CD if and only if the corresponding multiple of PQ exceeds the corresponding multiple of RS. Less cryptically,

if m and n are positive integers then mAB>nCD if and only if mPQ>nRS.

For $x, y \in S$ pick segments AB and CD such that $[AB] = x$ and $[CD] = y$. Define

$$\frac{x}{y}$$

to be the set of all ratios $\simeq$ to AB:CD.

Passing to segments classes $x, y, z, w \in S$, we declare (Elements Book V, Definition 5) that

$$\frac{x}{y} \simeq \frac{w}{z}$$

if the following holds:

for positive integers m and n, the condition $mx > ny$ holds if and only if $mw > nz$ holds.

We define x/y is less or equal to w/z,

$$\frac{x}{y} \leq \frac{w}{z}$$

if the following holds:

for positive integers m and n, if the condition $mx > ny$ holds then $mw > nz$ holds.

This is essentially Definition 7 in Euclid's Elements Book V.

The notion of ratio of segments shows that there is a natural relation between pairs of numbers (n, m) : we say that (n, m) and (p, q) correspond to the same *rational* if they measure the ratio of the same pair of segments, i.e. there are segments x and y such that

$$nx = my, \qquad \text{and} \qquad px = qy.$$

In fact we can just define the rational

$$\frac{n}{m}$$

to be the ratio $x : y$.

Notice that a *general ratio* $x:y$, as described by Euclid, *is specified by all rationals greater than* $x:y$ *and all rational less than* $x:y$. This is the essential first step in the construction of the real number system by Dedekind (1831 –1916).

Euclid presents numerous results concerning proportions. For example,

AB:CD=PQ:QR if and only if AB:PQ=CD:QR.

Moreover,

if AB:CD=PQ:RS and CD:EF=RS:TV then AB:EF=PQ:TV.

One of Euclid's theorems on triangles declares that if two triangles ABC and PQR have congruent angles, i.e. if $\langle ABC = \langle PQR$ and $\langle ACB = \langle PRQ$, then the sides are proportional, i.e.

AB:AC=PQ:PR, and AB:BC =PQ:QR, and AC:BC=PR:QR.

This is a key fact in the development of the algebra of proportions.

If $x,y,z \in S$ consider a triangle ABC with two sides given by $[AB] = x$ and $[AC] = y$. On the ray $\vec{AC}$ there is a unique point D such that $z = [AD]$. Now let E be the point on $\vec{AB}$ such that DE is parallel to BC. Then we define

$$\frac{x}{y}z \stackrel{\text{def}}{=} [AE].$$

Using this we can define the product of two ratios x/y and z/w as

$$\frac{x}{y}\cdot\frac{z}{w} = \frac{\frac{x}{y}z}{w}. \tag{3.1}$$

Now we can define the sum of two ratios:

$$\frac{x}{y}+\frac{z}{w} = \frac{x+\frac{z}{w}y}{y}. \tag{3.2}$$

A lengthy set of arguments now establishes the usual properties of addition and multiplication. Let 1 denote the ratio x/x:

$$1 \stackrel{\text{def}}{=} \frac{x}{x} \tag{3.3}$$

for any $x \in S$. Then

$$\begin{aligned} s+t &= t+s \\ s+(t+u) &= (s+t)+u \\ st &= ts \\ s(tu) &= (st)y \\ s(t+u) &= su+tu \\ \frac{x}{y}\cdot 1 &= \frac{x}{y} \\ \frac{x}{y}\cdot\frac{y}{x} &= 1. \end{aligned} \tag{3.4}$$

In proving these, the similar-triangles theorem is invaluable.

It is now possible to adjoin to the collection of all ratios an element 0 serving as additive identity:

$$s+0=s$$

and the 'negative' $-s$ for every ratio s. This yields a *field*.

With the Dedekind axiom of completeness (or, equivalently, the Hilbert maximality axiom) included, the field produced is identified as the real number system **R**.

We refer also to Hilbert [1] for alternative constructions of the algebraic operations. It is important to observe that it is possible to construct a division algebra structure (a field in all apsects except that multiplication is not necessarily commutative) by avoiding the axioms of congruence and continuity.

Thus, the 'pure geometry' constructed with axioms leads to an algebraic system.

Here are some summary observations:

1. By fixing any one segment AB as a 'unit', we can define the *length* of a segment CD to be the ratio $\frac{[CD]}{[AB]}$.

2. We can establish a 'coordinate system' for the plane. Fix two distinct non-opposite rays $\vec{OA}$ and $\vec{OB}$, with a common vertex O, and a point A on $\vec{OA}$. Take $[OA]$ as the unit segment to measure lengths, and think of $\vec{OA}$ and $\vec{OB}$ as the x-axis and y-axis, respectively. Then the set of all points in the plane is put into one-to-one correspondence with $\mathbf{R}^2$, the set of all ordered pairs of real numbers.

3. The operations of addition, subtraction, multiplication and division can be executed through ruler and compass constructions. Thus, we can start with any given set of points, say two points, consider all constructible points and segments; the ratios of the latter yield a field.

4. As noted earlier, the Eudoxus method of ratios is for ‘like magnitudes’, not only segments. Considering all rectangles R and S in the plane, we can define R:S by, for example, decomposing S into small enough congruent squares and counting how many copies of that can be used to approximate R. As in Item 1, fix a ‘unit’ segment AB. We can measure the *area* of the rectangle S by the ratio $S : U$, where U is the unit square, having sides congruent to AB. There is a relationship between ratios of segments and areas: a rectangle with sides given by segments x and y has the same area as a rectangle with sides z and w if and only if $x/w = z/y$.

5. The method of measuring areas in Item 4 can be extended to other polygonal figures, and even to other regions. Archimedes showed that the area enclosed by a circle is proportional to th square of the radius (πr^2), by constructed polygonal figures contained inside, and containing, the circular region. Further refinement of this idea leads the the theory of Riemann integration as well as of Lebesgue and Haudorff measures.

6. The ideas used for measuring areas go over to volumes, but there are greater difficulties if one insists on using the method of decomposing a polyhedron into other ones in order to measure volume. However, the Lebesgue measure theory works perfectly well in any (finite) dimension.

Problem Set 5

In the following, using the Hilbert axioms where needed. Do not use any other axioms.

1. Show that in the incidence geometry for 3 points there are no parallel lines.

2. Show that in the incidence geometry for 5 points there exist three lines l, m, and n, such that $l \| m$, and $m \| n$, but $l \not\| n$. (The notation $a \| b$ means ‘a is parallel to b.)

3. A *pencil* is a set consisting of a line along with all lines parallel to this. Count the number of pencils in the geometry with 4 points.

4. Using the axioms of incidence show that if A is a point and l a line not through A then there is a point B on the other side of l from A (i.e. l crosses the segment of $\overline{AB}$).

5. Prove the following results about line segments:

   (i) If AB is a segment then there is no point C between A and B for which AC is congruent to AB.

   (ii) If AB>CD then CD is not greater than AB.

   (iii) If AB>CD and CD>EF then AB>EF.

Bibliography

[1] Hilbert, David. 1956. *Grundlagen der Geometrie.* (Eight Edition, with supplementary material and revisions by Paul Bernays.) H.G. Verlagsgesellschaft mbH, Stuttgart.