Chapter 1

Numbers

Since the earliest times man has sought to find patterns in Nature. What is the principle governing the waxing and waning of the moon, the wandering of the planets among the fixed stars? How do the lengths of a plucked harp string relate to musical tones? From such curiosity science is born.

Whether one believes that the natural numbers

1, 2, 3, 4, ...

exist in some "real" sense or creations of the human mind, one can seek patterns and relationships among them just as one can among physical phenomena. One such pattern is the division of numbers into even (2, 3, 4, 6, ...) and odd (1, 3, 4, 5, ...), or into squares (1, 4, 9, 16, ...) and non-squares (2, 3, 5, 6, ...). It is clear that there are infinitely many even numbers and infinitely many odd ones, and it is also clear that there are both infinitely many squares and infinitely many non-squares. Other patterns are much more subtle and still hold many puzzles. Consider, for example, the primes (2, 3, 5, 7, 11, ...). These are the whole numbers greater than 1 that cannot be factored, except in an obvious way. The whole numbers greater than 1 that are not prime are called *composite*. There are infinitely many of these, and the complete list begins with 4, 6, 8, 9, ...

Aside: We said that certain things are "clear" or "obvious." Is this really so? How would you back up these assertions if challenged?

Now let us ask, as the Greeks did,

How many primes are there?

This question is a deep one, and the answer is not obvious. However, the correct response, given by Euclid around 300 BC, is that are infinitely many. Here is his argument:

Suppose, on the contrary that there are just finitely many primes. Then we can list them:

$$p_1, p_2, \ldots, p_N.$$

The first prime is $p_1 = 2$, and the last prime is p_N. Now consider the number obtained by multiplying all the primes, then adding one:

$$Q = p_1 p_2 \cdots p_N + 1.$$

There are two possibilities. The first is that Q is prime, the second is that it is not, in which case Q is composite. In the first case Q is bigger than any of the listed primes. (Why?) But then we are faced with a contradiction, for we have produced a prime not on the list. Consider therefore the second case. If Q is not prime, it has factor less than Q but bigger than 1. In fact, it has a prime factor. (Why?) This factor is somewhere on the list. Let us suppose that it is the prime p_k. Now divide Q by p_k. The remainder is 1. (Why?) But this too is a contradiction, because when we divide a number by a factor, the remainder is zero.

Let us stand back and observe what conclusion we have reached. In either case the assumption "there are finitely many primes" has led to a contradiction. Therefore the fault lies with the assumption: it is false, and therefore its negation, "there are infinitely many primes," is true.

Let us stand back still further and consider how we reached our conclusion. For the theorem, "there are infinitely many primes," we have given a logically connected chain of sentences which bridge the gap from what we accept as certain to what we claim to know. This logical argument, a *proof*, is a certificate which guarantees the truth of the theorem. But it is something more as well: a kind of tightly edited record of the discovery of the theorem which gives us insight into *why* it is true.

The proof that there are infinitely many primes is "by contradiction." This is an intellectual tool pioneered by the Greeks, who thought deeply about truth and logic. We will use it again and again in what follows.

Euclid's theorem about primes should be contrasted with the standard Greek theory of astronomy, which was based on the idea that earth sits at (or near) the center of the universe, with the stars attached to a sphere which revolves once a day around that center. That idea (which fits our observations on a clear summer night) was rejected by Copernicus at the close of the sixteenth century, almost two millennia after Euclid: the earth revolves about the sun, and is not at rest in the universe. We know now that Copernicus was correct and the Greeks were not. However, the Greek theorem on primes, proved in Euclid's day, is true 2300 years later and is in fact eternally true. A proof is a very good certificate indeed.

Primes

Let's look for number patterns beyond those we have already seen — even and odd, square and nonsquare, prime and composite. A good place to start is with a closer look at the primes, and for this we need some "experimental data." To make a table of primes we could take each integer $n > 1$ in turn, factor it, and list the numbers that can't be factored. But there is a better way, the so-called *sieve of Eratosthenes*. (Eratosthenes, who worked in Alexandria, in northern Egypt, lived from about 276 BC to 195 BC. He is famous for his measurement of the circumference of the earth). Here is how the sieve works for primes less than or equal to 17. First write down the integers 2 ... 17:

```
2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
```

Then mark all the multiples of 2, except 2 itself:

```
2 3 *4 5 *6 7 *8 9 *10 11 *12 13 *14 15 *16 17
```

Then mark all multiples of the next unmarked number except that number itself. In the present case, that number is 3:

```
2 3 *4 5 *6 7 *8 *9 *10 11 *12 13 *14 *15 *16 17
```

In general, we continue until there is nothing left to mark; the numbers that remain unmarked are the primes. In the present case there is nothing left to do, and so the primes in question are

```
2, 3, 5, 7, 11, 13, 17
```

Using Eratosthenes' sieve it is not hard to make a table of the first one hundred primes:

```
  2    3    5    7   11   13   17   19   23   29
 31   37   41   43   47   53   59   61   67   71
 73   79   83   89   97  101  103  107  109  113
127  131  137  139  149  151  157  163  167  173
179  181  191  193  197  199  211  223  227  281
233  239  241  251  257  263  269  271  277  281
283  293  307  311  313  317  331  337  347  349
353  359  367  373  379  383  389  397  401  409
419  421  431  433  439  443  449  457  461  463
467  479  487  491  499  503  509  521  523  541
```

From the table you will notice that that primes occur somewhat irregularly, with the gaps between them tending to be larger for larger primes. You will

also notice that there are many primes for which the gap is very small: two units. Consider, for example, the primes 5 and 7, the primes 521 and 523. These pairs are "twin primes." When we look for larger and larger twin primes, we always find them. It is therefore natural to ask

Are there infinitely many twin primes?

The answer is unknown. Thus, while there seems to be an apparent pattern, we do not know for certain that it holds, and we do not understand why it should hold.

Here is another piece of experimental mathematics. Looking at our table of primes, we find many of the form "one plus a square," e.g., $5 = 2^2 + 1$ and $401 = 20^2 + 1$. It seems that whenever we look larger and larger special primes of this kind, we find them, e.g., $17957 = 134^2 + 1$. Thus it is natural to conjecture that there are infinitely many primes of the form "one plus a square." The answer to this conjecture is also unknown.

Pythagorean triples

Let us consider another question about numbers: "can a square number be divided into two squares?" Here is an example:

$$5^2 = 3^2 + 4^2$$

The square number 25 can be written as a sum of the two squares 9 and 16, corresponding to the geometric fact that there is a right triangle with sides 3, 4, and 5. Not all squares can be "divided into squares." This is the case, for example, for the number 36. (Prove this!)

The question we have just considered goes back at least as far as Diophantus, a Greek mathematician who worked in Alexandria around 250 AD. Put in modern form, we ask for positive integers which solve the equation

$$x^2 + y^2 = z^2. \tag{1.1}$$

A solution is called a *Pythagorean triple*; as the name suggests, it represents a right triangle. With a little experimentation, you can discover more solutions of (1.1). But the fundamental questions are these:

1. Are there infinitely many Pythagorean triples?
2. Is there formula for manufacturing Pythagorean triples?
3. Which squares can be written as a sum of two squares?

To formulate answers to these questions it will help to look at some data. In order to concentrate on the essentials, we do not list triples like (6,8,10) that

are multiples of other triples. The important ones are those, like (3,4,5), whose components have no common factors. We call them *primitive*. Below we list all the primitive triples such that $1 \leq x \leq y \leq z \leq 100$.

```
(3,4,5)       (5,12,13)     (8,15,17)     (7,24,25)
(20,21,29)    (12,35,37)    (9,40,41)     (28,48,53)
(11,60,61)    (16,63,65)    (33,56,65)    (48,55,73)
(13,84,85)    (36,77,85)    (39,80,89)    (65,72,97)
```

It is easy to check that each of the sixteen triples above is Pythagorean. But how do we know that we have not missed one? For this we used a short computer program `ptripleseach` which is listed at the end of this chapter. Note that the triples are listed in increasing order of the "hypotenuse," z. The list of z-values is

```
5, 13, 17, 25, 29, 37, 41, 53, 61, 65, 65, 73, 85, 85, 89, 97
```

Is this a sequence that can be understood?

Diophantine Equations

An equation with integer coefficients for which we seek integer (or sometimes rational) solutions is called *Diophantine*. The prototype is the Pythagorean triplet equation (1.1). Let us look at a other examples, beginning with the equation.

$$111x - 119y = 1 \tag{1.2}$$

Its real solutions are easy to understand: they comprise a straight line, as in figure 1 below. But are there integer solutions? Yes, because the following "integer vector" works: (104, 97). But are there other solutions? Are there finitely or infinitely many solutions? Is there a method for computing solutions? We will study these questions in the next chapter.

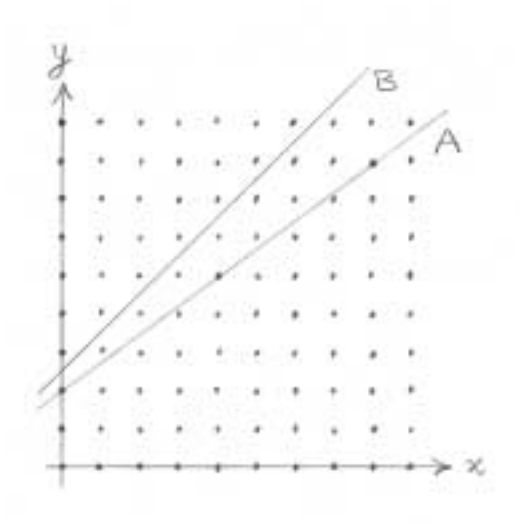

Figure 1: $ax + by = c$

Consider next the equation

$$x^2 - 2y^2 = 1. \tag{1.3}$$

Its real solutions form a hyperbola, and the Diophantine problem is to find those which have integer coordinates. A closely related equation is

$$x^2 - 4y^2 = 1? \tag{1.4}$$

How do its integer solutions compare with those of the previous equation? We will study these questions in chapter 4.

Finally, consider the cubic equation

$$x^3 + y^3 = z^3 \tag{1.5}$$

which is the algebraic form of the question "can a cube be divided into two cubes?" There are some trivial solutions, such as $(1, 0, 1)$ and a few others with one coordinate zero. But are there any positive integer solutions? It turns out that there are none. This is a difficult result which is a special case of *Fermat's conjecture*: *the equation*

$$x^d + y^d = z^d \tag{1.6}$$

has no integer solutions with all coordinates positive, provided $d > 2$. We know of the conjecture from a marginal note that Fermat, a French judge and mathematician (1601-1665), wrote in his copy of Diophantus' *Arithmetica*. The conjecture was finally solved by Andrew Wiles of Princeton University in 1995. Not all problems were formulated (or solved) by the Greeks!

Problems

Evens and Odds, and Mods and Squares

1. Prove that the square of an even number is even, and that the square of an odd number is odd.

2. Take a whole number a and square it. What are the possible values of the remainder when you divide it by two? Answer the same question when you divide it by $N = 3$ and by $N = 4$.

3. If r is the remainder we get when we divide a by N, we say that $a = r \bmod N$. Thus $7 \bmod 3 = 1$ and $8 \bmod 3 = 2$. If we change the modulus, we get different results: $7 \bmod 4 = 3$ and $8 \bmod 4 = 0$. What is $12345 \bmod 171$? What is $54321 \bmod 171$. What is

$$12345 \times 54321 \bmod 171?$$

   Is there a pattern to be discovered here? Are there other patterns?

4. We can make the remainders that we get when we divide by N into a little system of arithmetic, called "arithmetic mod N." To add two numbers mod N, we add them in the usual way, then take the remainder mod N. We do the same for multiplication: multiply in the usual way, then take the remainder mod N. Below are the addition and multiplication tables mod 3. Find the corresponding tables mod 2, 4 and 5.

```
+  | 0 1 2        x | 0 1 2
-----------       ---------
 0 | 0 1 2        0 | 0 0 0
 1 | 1 2 0        1 | 0 1 2
 2 | 2 0 1        2 | 0 2 1
```

   Whe you finish your tables, see if you see any interesting patterns.

5. Find an x so that equation $x + 2 = 0 \bmod 5$. Then find a y so that $2y = 1 \bmod 5$.

   By an equation $a = b \bmod 5$, we mean that when we "reduce mod 5," we get the same thing on the left as we do on the right. Thus $12 = 22 \bmod 5$.

6. Can every whole number be written as a sum of two squares? Does this question lead you to discover any patterns?

Rationals and Irrationals

7. A number is *rational* if it can be written as a ratio of integers: it is a fraction, like 2/3. If a number cannot be written as a fraction, it is called

irrational. Are there any such numbers? Let's consider the square root of 2. If it is rational, we can write $\sqrt{2} = a/b$, where the fraction a/b is in lowest terms (no factor common to the numerator and denominator. From this we deduce that $a^2 = 2b^2$. Now use the result of the previous problem about squares of even an odd numbers. The argument and result you will discover is recorded in the dialogue *Thaetetus* of Plato (ca. 428–347 BC).

8. Prove that $\sqrt{3}$ is irrational. What is the general result. Can you prove that it is true?

   Remember: a good proof = a good understanding

9. What are the decimal expansions of 1/125 and 1/7? What about 13/12 and 13/11? Can you make a general statement about the decimal expansion of rational numbers based on these examples and others like them? Can you prove the general statement?

10. Show that 0.333... is rational. Then show the same for 0.123123123.... (We use the notation $0.\overline{123}$ for repeating decimals; thus $12.98\overline{577}$ is an *eventuall repeating* decimal). Can you formulate a general statement? Can you prove that it is true?

Sequences and Limits

11. Consider the number $\alpha = 0.101001000100001...$ (written in binary)! We could also write it as

$$\alpha = \frac{1}{2} + \frac{1}{2^3} + \frac{1}{2^6} + \frac{1}{2^{10}} + \frac{1}{2^{15}} + \cdots$$

    What are the next two terms of the infinite series above? (Discover and extend the pattern). Is α rational or irrational?

    Notice that the binary or decimal expansion of a number is really an infinite series. In the case of the number α, the "partial sums of the series" are

$$\alpha_1 = 1/2,\ \alpha_2 = 1/2 + 1/8,\ \alpha_3 = 1 + 1/8 + 1/64,\ \textit{etc.}$$

    Thus

$$\alpha_1 = 1/2,\ \alpha_2 = 5/8,\ \alpha_3 = 41/64,\ \alpha_4 = 657/1024,\ \textit{etc.}$$

    What are α_5 and α_6?

    The rational numbers α_n give better and better approximations to α itself: we say that the sequence $\{\ \alpha_n\ \}$ tends to the limit α, and we write

$$\lim_{n\to\infty} \alpha_n = \alpha.$$

12. Consider the "mystery sequence" defined as follows: $x_1 = 1$ and

$$x_{n+1} = \frac{1}{2}\left(\frac{3}{x_n} + x_n\right) \tag{1.7}$$

Compute the first five terms of the sequence. Does the sequence have a limit? If so, what is the limit? Can you prove the assertions you make?

What happens when we change the *initial value* x_1 which generates the sequence $\{\ x_n\ \}$ defined by (1.7).

Note: a relation like $x_{n+1} = f(x_n)$ for some function f is called a *recursion relation.*

13. What can you say about the decimal expansion of $\sqrt{2}$?

14. Let $\{z\}$ denote the fractional part of z. Thus $\{3.1416\} = 0.1416$ and $\{22/7\} = 1/7$. Study the sequence of numbers $x_k = \{k\sqrt{2}\}$ for $k = 1, 2, 3, , \ldots$. Do you see any patterns? Can the sequence be *periodic*, that is, eventually repeat itself? Compare the sequence x_k with the one defined by $y_k = \{(1117/1009)k\}$.

For this problem you should use a calculator, ordinary or programmable. You can also use the Maple code listed at the end of this section.

15. Consider the *very* mysterious sequence

```
1, 2, 1/2, 1/3, 3, 4, 3/2, 2/3, 1/4, 1/5,
5, 6, 5/2, 4/3, 3/4, 2/5, 1/6, ...
```

What are the next four terms? Can this sequence be understood? Is there a formula or algorithm for generating it?

16. Sequences like (x_k) and (y_k) can be studied for their statistical properties. For example, we can compute the frequency with which the terms $x_1, \ldots, x_n$ lie in the interval $[a, b] = \{\ x\ \mid a \le x \le b\ \}$:

$$F(n, a, b) = \frac{\text{number of } k \le n \text{ such that } a \le x_k \le b}{n}$$

Examine the behavior of $F(n, 0, 1/2)$ as n becomes larger and larger. Do the same for $F(n, 0, 1/3)$, etc.

Primes

17. Make a list of primes $p \le 100$ using the sieve of Eratosthenes. Do this with pencil and paper. How many are there?

18. List the primes as p_1, p_2, p_3, ... and let $Q_k = p_1 p_2 \cdots p_k + 1$. Is Q_k always prime?

19. Consider the polynomial $f(n) = n^2 + n + 41$. What can you say about the sequence $f(0)$, $f(1)$, $f(2)$, ...?

20. Let $N(x)$ be the number of primes $p \leq x$. Big project: understand $N(x)$. (Perhaps tables and graphs will lead to some ideas).

21. Factor the numbers 1234, 1235, 1236, 1237 into primes. Do this with pencil, paper, and basic calculator. (For us a basic calculator does addition, subtraction, multiplication, division, and extraction of square roots).

22. Describe the method you use to factor an integer. It should be a step-by-step recipe (algorithm) that could be carried out by a clerk with no skills other than arithmetic and the ability to follow directions. We'll let the clerk use a basic calculator.

23. If n is composite, how large can its smallest factor be? Think about examples, if necessary, or use pure thought. Then formulate a result and prove that it is true.

24. Consider the sequence of numbers $M_p = 2^p - 1$, where p is prime. What can you say about this sequence?

25. In the proof that there are infinitely many primes, we used the assertion "if a postive integer has a factor, then it has a prime factor." Prove this assertion.

26. Study the gaps between primes. Is there any visible pattern? Can the gaps between primes be arbitrarily large? How does the "average size of a gap" behave as one moves further and further into the list of primes?

27. Let $F(p, n)$ be the relative number of integers in the sequence 2, 3, 4, 5, ..., n which are not divisible by the prime p:

$$F(p, n) = \frac{\text{number of integers } k\text{: } 2 \leq k \leq n, \text{ not divisible by } p}{n - 1}$$

Then $F(2, n) \approx 1/2$ when n is large. (We say that "$a \approx b$" if a is approximately equal to b). Find a simple approximate formula for $F(p, n)$ for the other primes. Now let $F(2, 3, n)$ be the relative number of integers 2, 3, ... n which have no factors in common with 2 *and* 3. Find a simple approximate formula for this quantity. Generalize to $F(2, 3, 5, n)$, etc.

Pythagorean Triplets & Diophantine Equations

28. What patterns do you see in the table of Pythagorean triplets?

29. Prove that there is no right triangle with integer sides and hypotenuse 6. Do the same for hypotenuse 7.

30. If $x^2 + y^2 = z^2$ is a Pythagorean triple, then we have the factorizations $x^2 = z^2 - y^2 = (z + y) \cdot (z - y)$ and also $y^2 = z^2 - x^2 = (z + x) \cdot (z - x)$. Using the data in the table above, see if you can find any patterns in these factorizations.

31. Consider the line A in Figure 1 above. What is its equation? (Write it with integer coefficients).

    An integer vector (x, y) like $(3, 4)$ is a potential solution to a Diophantine equation like $17x - 31y = 1$. Are there Diophantine equations that have no integer solutions? What would the corresponding geometric picture be?

32. You do not yet know methods for solving Diophantine equations. Nonetheless, try to find solutions to (a) $3x + 5y = 1$, (b) $11x + 4y = 1$, (c) $91x + 104y = 1$. These are linear equations (consider their graphs). Try also the quadratic equations (d) $x^2 + 2y^2 = 11$, (e) $x^2 - 2y^2 = 1$. (Consider their graphs).

33. Make up your own problem/question and try to solve/answer it.

    An intellectual discipline advances when someone answers one of its important questions, e.g., why does the moon circle the earth? But for us to get even that far, someone must have the insight to ask the right question. Questions are as important as answers. Perhaps more important, since one precedes the other.

Computer projects

Below we give some programs written in Maple which can be used to explore questions about numbers. For the moment, try them as is. Then read through the Maple code and try to get a sense of how it works. This will give you a basis for writing your own programs.

Sequences

We give some general tools for studying sequences of numbers, e.g., the sequence of primes. To count the number of primes which satisfy the inequality $a \leq p \leq b$, we use the function

```
countprimes := proc(a,b)
   local i, N;
   N := 0;
   for i from a to b do
      if isprime(i)
        then N := N + 1;
```

```
      fi;
   od;
   RETURN( N );
end;
```

For example, if we say `count(2,100)` then we find the number of primes between 2 and 100. (See the note below for a few words on how the built-in Maple function `isprime` works).

Now suppose we want to study the sequence $f_k = \{k\sqrt{2}\}$, where $\{x\}$ is the fractional part of x, e.g., $\{3,1416\} = 0.1416$. For this we define the function

```
f := k -> frac( evalf( k*sqrt(2) ) );
```

To generate part of the sequence, we can say this:

```
 for i from 1 to 20 do
    print( i, f(i) );
  od;
```

However, it is diffcult to make much sense of long sequences without other tools. Thus we design a function to count the number of terms in the sequence $f_1, \ldots, f_n$ which satisfy the inequality $a \leq f_k \leq b$:

```
countseq := proc(f,n,a,b)
    local i, N;
    N := 0;
    for i from 1 to n do
       if ( a <= f(i) ) and ( f(i) <= b )
          then N := N + 1;
       fi;
    od;
    RETURN( N );
end;
```

It is also useful to consider the relative frequency with which elements of the sequence $f_1, \ldots, f_n$ satisfy the inequality $a \leq f_k \leq b$. If there are N of these, then the relative frequency is N/n. Here is a Maple function which computes the relative frequency:

```
freq := proc(f,n,a,b)
    local i, N;
    N := 0;
    for i from 1 to n do
       if ( a <= f(i) ) and ( f(i) <= b )
          then N := N + 1;
```

```
      fi;
    od;
    RETURN( evalf(N/n) );
end;
```

Note. The following quote from the Maple help system (obtained by typing `?isprime`) sheds some line on how `isprime works`.

> The function `isprime` is a probabilistic primality testing routine.
>
> It returns false if n is shown to be composite within one strong pseudo-primality test and one Lucas test and returns true otherwise. If `isprime` returns true, n is "very probably" prime - see Knuth "The art of computer programming", Vol 2, 2nd edition, Section 4.5.4, Algorithm P for a reference and H. Reisel, "Prime numbers and computer methods for factorization". No counter example is known and it has been conjectured that such a counter example must be hundreds of digits long.

We will learn something about probabilistic primality testing later. (See also [2], ch XX.). In the mean time you may wish to devise an algorithm, maybe even a program for factoring an integer into primes. Thus if it finds only one factor, the given number is prime.

Twin primes

The function `twinsearch(a,b)` lists pairs of twin primes in the interval $a \leq p \leq b$ and returns the number in that interval. How good is the experimental evidence for the twin primes conjecture?

```
twinsearch := proc(a,b)
  local i, count;
  count := 0;
  for i from a to b do
    if isprime(i) and isprime(i+2)
       then  print(i, i+2 );
        count := count + 1;
    fi;
  od;
  RETURN( count );
end;
```

Primes of the form $N^2 + 1$

Use the function `spsearch(a,b)` investigate the occurence of "special primes" of the form $N^2 + 1$ in the interval $[a, b]$.

```
spsearch := proc(a,b)
    local i, count;
    count := 0;
    for i from a to b do
      if isprime(i) then
        if i = (trunc(sqrt(i)))^2 + 1 then
          print(i);
          count := count + 1;
        fi;
      fi;
    od;
  RETURN (count );
end;
```

Pythagorean triplets

The function `ptriplesearch(a,b)` prints the primitive Pythagorean triplets i, j, k satisfying $a \leq i \leq j \leq k \leq b$ and returns the number of triples found. You can use it to investigate the properties of Pythagorean triples.

```
ptriplesearch := proc(a,b)
  local i,j,k,count;
    count := 0;
    for i from a to b do
      for j from i to b do
        for k from j to b do
          if  i^2 + j^2 = k^2 and gcd(i,j) = 1
            then
               print( i, j, k );
               count := count + 1;
          fi;
        od;
      od;
    od;
  RETURN( count );
end;
```

Diophantine equations

The function `diosearch(f,a,b)` prints out solutions of $f(i, j) = 0$ where $0 \leq i \leq a$ and $0 \leq j \leq b$, and it returns the number of solutions found.

```
diosearch := proc(f,a,b)
   local i, j, count;
```

```
   count := 0;
   for i from 0 to a do
      for j from 0 to b do
         if f(i,j) = 0 then
           print( i, j );
           count := count + 1;
         fi;
      od;
   od;
   RETURN( count );
end;
```

To use `diosearch`, you must define the function f. If we want to investigate Pell's equation, $x^2 - 2y^2 = 1$, we make the definition

```
f := (x,y) -> x^2 - 2*y^2 - 1;
```

Of course, we can define all sorts of functions, e.g.,

```
g := (x,y) -> y^2 - x^3 - 17;
```

Then you can say `diosearch(g,100,100)` to find all integer solutions of $y^2 = x^3 + 17$ such that $0 \le x \le 100$ and $0 \le y \le 100$.

Notes

Logic

In the problems above we made informal use of certain principles of logic. It is worthwhile to study them formally.

The Converse

In problem 9 above, you showed that if a number x is rational, then its decimal expansion is eventually repeating, e.g., $1234/101 = 12.\overline{2178}$. Note the form of this statement:

> If P then Q.

Thus P = "if a number is rational," and Q = "its decimal expansion is eventually repeating." Now consider the statement

> If Q then P.

It is called the *converse* of the original statement. In the case at hand the converse is a true statement. This is what you proved in problem 10: "if a number has an eventually repeating decimal expansion, then it is rational." Note that the truth of a statement does not automatically imply the truth of its converse. Consider, for example, the assertion "if it is raining, then there are clouds in the sky." This is always true. However, the converse, "if there are clouds in the sky, then it is raining," may or may not be true. Thus a statement and its converse are not logically equivalent: one can be true, the other false.

Statements of the form "if P then Q" are called *implications*, and we sometimes say "P implies Q." When we say

> P if and only if Q

we really mean "if P then Q" *and* "if Q then P."

> A number is rational and only if its decimal expansion is eventually repeating.

The Contrapositive

Consider once again the implication

> If P then Q.

Its *contrapositive* is

> If not-Q then not-P.

An implication is logically equivalent to its contrapositive: either both are true or both are false. Consider, for example, the assertion "if it is raining, then there are clouds in the sky." Its contrapositive is "if there are no clouds in the sky." Consider also the statement "if a number is rational, then its decimal expansion is eventually repeating." Its contrapositive is "if the decimal expansion of a number is not eventually repeating, then it is not rational." Using this assertion we can resolve problem 11. Likewise, the contrapositive of the assertion "if the decimal expansion of a number is eventually repeating, then it is rational," resolves problem 13.

History

(1) The Greeks were a lively and argumentative lot. This is perhaps why they discovered the idea proof: as with debates and courts of law, proofs are a way of settling arguments.

Notation, Number Systems, and Sets

Mathematicians have come to love the use of symbols to stand for all sorts of things, not just numbers like 1, 2, 3, etc. For example, the use $\mathbf{N}$ to denote the set of *natural* numbers:

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

The natural numbers are the positive "whole" numbers: the ones we count with. The set of numbers

$$\mathbf{Z} = \{\ \ldots -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ \ldots\ \}$$

is called the "integers." Latin, *integer* means "whole," or "untouched" (from *in-tangere*, like "intangible"). The use of the letter "Z" comes from the German "Zahl," which means "number." For the set of rational numbers, alias ratios of integers, alias fractions, we use the symbol $\mathbf{Q}$. Latin *frangere* means "to break;" its past participle is *fractus*, "broken." A fraction is a broken number, or a piece of a whole. Why the letter "Q?" It probably comes from "quotient." We use $\mathbf{R}$ for the set of real numbers and $\mathbf{C}$ for the set of complex numbers. The numbers $\sqrt{2}$ and π are real but not rational. The numbers $\sqrt{-1}$ and $2+3\sqrt{-1}$ are complex but not real. The number $i = \sqrt{-1}$ is "imaginary." One should this term of this as a statement about the creativity of those who first thought of such numbers, not a statement about their supposed unreality. (Quantum mechanics, which is the physical theory that explains atoms and light, deals with very real objects. The mathematics on which this theory depends uses complex numbers in an essential way.)

We have repeatedly used the word "set." A set is just a collection of elements. For example, both $\{\ 1, 2, 3, 4\ \}$ and $\{\ \spadesuit, \clubsuit, \heartsuit, \diamondsuit\ \}$ are sets. These two sets happen to be in *one-to-one correspondence*. These means that we can pair the elements of one set with the elements of the other set with no elements left over:

$$1 \longleftrightarrow \spadesuit$$
$$2 \longleftrightarrow \clubsuit$$
$$3 \longleftrightarrow \heartsuit$$
$$4 \longleftrightarrow \diamondsuit$$

Supplementary problems

1. Let $a = 3+4\sqrt{-1}$, $b = 1-\sqrt{-1}$. Compute $a+b$, $a-b$, ab, and a/b. Then plot all six numbers in the complex plane.

2. The *conjugate* of $z = x+y\sqrt{-1}$ is $x-y\sqrt{-1}$, which we write as $\bar{z}$. Compute $a \cdot \bar{a}$ and $b \cdot \bar{b}$. Interpret these quantities geometrically. (We write $|a|^2$ for $a \cdot \bar{a}$).

3. How many one-to-one correspondences are there between the sets $\{\ 1, 2, 3, 4\ \}$ and $\{\ \spadesuit, \clubsuit, \heartsuit, \diamondsuit\ \}$?

4. Show that the set of positive integers is in one-to-one correspondence with the set of even positive integers. This fact, which is one of the seemingly paradoxical properties of infinite sets, was known to the Italian mathematician and physicist Galileo (1564-1642).

5. How should we define the notion "infinite set?"

6. Show that the set of positive integers is in one-to-one correspondence with the set of squares.

7. Is the set of positive integers in one-to-one correspondence with the set of positive rational numbers? This question was raised (and settled) by the German mathematician Georg Cantor (1845-1918).