Excursions in Computing Science:
Week i. Rules and Calculations

T. H. Merrett[*]
McGill University, Montreal, Canada

July 23, 2019

I. Prefatory Notes

1. Rules and sums. Teacher, invite your grade scholar to check some of the following rules and continue them up to, say, 13. The "rules" are given in the leftmost column and calculations up to 5 follow. Explain the meaning of Σ and let your pupil write in heir notebook the terms integer, positive integer, triangle number, odd number, square number, tetrahedral number, pyramidal number and cubic number, depending on how far hey gets. (There is even a 4-dimensional simplex of five points, each connected to each other, in the second-last line.)

Your grade scholar should get to know at least the triangle, square, tetrahedral and cubic numbers as well as the positive integers. A keen pupil will be eager to calculate, and will be interested in the relationships among these kinds of number. By all means offer a calculator. (I've been using a 1994 Texas Instruments TI81, which has variables, graphics and is programmable, but lots of others are even better. The main material later in *Excursions in Computing Science* is developed in the MATLAB® language, so that is also an alternative, albeit more sophisticated.)

(Be prepared for digressions if you offer your grade scholar a calculator as powerful as the programmable graphics calculators I am suggesting. Hey will want to explore all the other buttons, too.)

You and your grade scholar can take this material at a number of different levels. The simplest, for example, would be just to explore the calculations started below, without attempting to understand the patterns. This could provide experience to be amplified later by second and third passes through the material.

[*] The author gratefully acknowledges support from the taxpayers of Québec and of Canada who have paid his salary and research grants while this work was developed at McGill University, and from his students and their funding agencies. The present Notes are based on the teaching and ideas of Eugene Lehman.

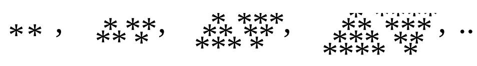
n	1	2	3	4	5	··
$\sum_n$	1	3	6	10	15	··
$\triangle_n$	*	* **	* ** ***	* ** *** ****	* ** *** **** *****	··
$n(n+1)/2$	1	3	6	10	15	··
$2n-1$	1	3	5	7	9	··
odd	*	** *	*** * *	**** * * *	***** * * * *	··
$\sum 2n-1$	1	4	9	16	25	··
$\square_n$	*	** **	*** *** ***	**** **** **** ****	***** ***** ***** ***** *****	··
n^2	1	4	9	16	25	··
$n+2\triangle_{n-1}$	1	4	9	16	25	··
$\sum\triangle_n$	1	4	10	20	35	··
▱$_n$	*	* * **	* * ** * ** ***	* * ** * ** *** * ** *** ****	* * ** * ** *** * ** *** **** * ** *** **** *****	··
$n(n+1)(n+2)/6$	1	4	10	20	35	··

n	1	2	3	4	5	..
◭$_n$	*	* ** **	* ** ** *** *** ***	* ** ** *** *** *** **** **** **** ****	* ** ** *** *** *** **** **** **** **** ***** ***** ***** ***** *****	..
$\sum$□$_n$	1	5	14	30	55	..
△$_n$+2▱$_{n-1}$	1	5	14	30	55	..
$n(n+1/2)(n+1)/3$	1	5	14	30	55	..
⬡$_n$	*	** *** **	*** **** ***** **** ***	**** ***** ****** ******* ****** ***** ****	..	
	1	7	19	37	61	..
$\sum$ ⬡$_n$	1	8	27	64	125	..
⬢$_n$, ⧉$_n$, n^3	1	8	27	64	125	..
n+6△$_{n-1}$+6 ▱$_{n-2}$	1	8	27	64	125	..
$\sum$ ⧉$_n$	1	9	36	100	225	..
△$_n$+6▱$_{n-1}$+6 ⬠$_{n-2}$	1	9	36	100	225	..
△$_n^2$	1	9	36	100	225	..

2. Some visualizations. Here are some visual intuitions behind the sameness of some of the rows in the sum tables.

Why is the nth triangle number $n(n+1)/2$? Here is a n by $n+1$ "rectangle" (parallelogram) made from two triangles.

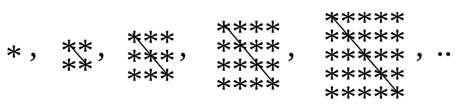
$\sum n$ = (△$_n$+▽$_n$)/2:



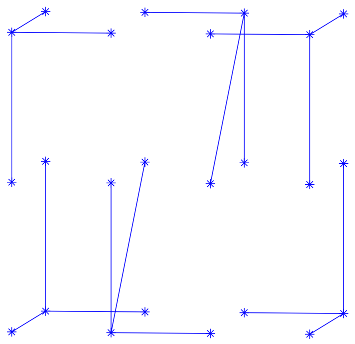
= $n(n+1)/2$

Why is $n^2 = n + 2\Delta_{n-1}$?

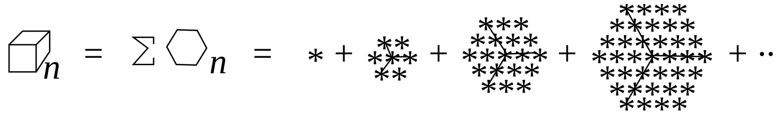
□$_n$ = n + 2△$_{n-1}$:



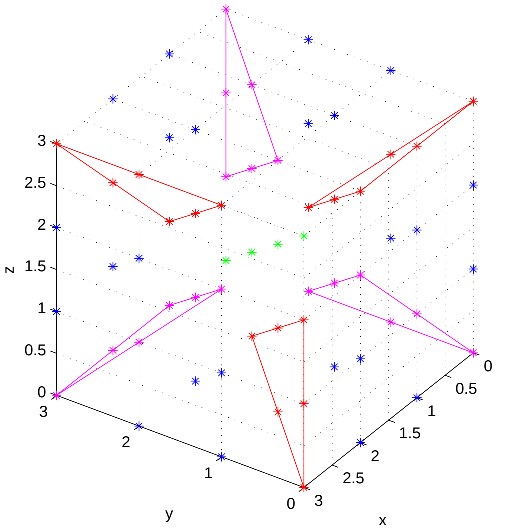
Why is the nth tetrahedral number $n(n+1)(n+2)/6$? Here is a n by $n+1$ by $n+2$ hexahedron (rectangular "cube") made from six tetrahedra.



Why do hexagonal numbers sum to cubes?



Why is $n^3 = n + 6\Delta_{n-1} + 6\,⟠_{n-2}$? (The symbol for tetrahedral numbers is slightly modified to ⟠.)



3. Rules and differences

n	1	2	3	4	5	··
$(n+1)-n$	1	1	1	1		··
n^2	1	4	9	16	25	··
$\mathrm{diff}_2(n)=(n+1)^2-n^2$	3	5	7	9		··
$\mathrm{diff}_2^2(n)=\mathrm{diff}_2(n+1)-\mathrm{diff}_2(n)$	2	2	2			··
n^3	1	8	27	64	125	··
$\mathrm{diff}_3(n)=(n+1)^3-n^3$	7	19	37	61		··
$\mathrm{diff}_3^2(n)=\mathrm{diff}_3(n+1)-\mathrm{diff}_3(n)$	12	18	24			··
$\mathrm{diff}_3^3(n)=\mathrm{diff}_3^2(n+1)-\mathrm{diff}_3^2(n)$	6	6				··
$\triangle_n^2-\triangle_{n-1}^2$		8	27	64	125	··
$\square_n-\square_{n-1}$		7	19	37	61	··

4. Rules and programming. We can use a programmable calculator to find the numbers in the sum and difference tables. Here are two programs for the TI81, followed by a brief explanation of how to enter and run the first.

```
Prgm1:  TRIANGLE
Input N
N*(N+1)/2 →T
Disp T
```

```
Prgm2:  TETRAHED
Input N
N*(N+1)*(N+2)/6 →T
Disp T
```

Creating `Prgm1`:
`PRGM` button; select `EDIT`; `ENTER` button.
Type `T R I A N G L E`; `ENTER` button.
`PRGM` button; select `I/O`; select `Input`; `ENTER`.
`ALPHA` button; type `N`; `ENTER`.

ALPHA button; type N; type * (
ALPHA button; type N; type + 1) / 2
STO button; ALPHA button; type T
PRGM button; select I/O; select Disp; ENTER.
ALPHA button; type T
QUIT button (2nd QUIT).

Running Prgm1:
PRGM button; select EDIT; ENTER button.
ENTER button.
After the prompt (?) enter a number (e.g., 5) and ENTER
The answer appears (e.g., 15).

Here are the same two programs written in MATLAB.

```
% function t = triangle(n)      THM      080708
% (In file triangle.m)
% find triangle number n
function t = triangle(n)
t = n*(n+1)/2;


% function t = tetrahed(n)      THM      080708
% (In file tetrahed.m)
% find tetrahedral number n
function t = tetrahed(n)
t = n*(n+1)*(n+2)/6;
```

To run the first, in MATLAB's Command Window write, say

```
triangle(3)
```

and the response is

```
ans =
                                 6
```

These programs should not need explanation. Here is a fancier one.

On the TI81

```
Prgm3:  SUMN
Input N
N→S
Lbl L
N − 1→N
If N = 0
Goto F
S + N→S
Goto L
Lbl F
Disp S
```

where to enter the label Lbl L from the EDIT PRGM state:
PRGM button; select CTL; select Lbl; ENTER
ALPHA button; type L

and to enter the condition If N = 0 from the EDIT PRGM state:
PRGM button; select CTL; select If; ENTER

`ALPHA` button; type `N`
select `TEST` button; select `=`; `ENTER`; type `0`

What this does is: if the condition (`N = 0`) is true, execute the next line (`Goto F`), otherwise skip that line and execute the following line.

Finally, to enter the control transfer, `Goto F`:
`PRGM` button; select `CTL`; select `Goto`; `ENTER`
`ALPHA` button; type `F`

which will jump the running program to the label `F` at the end (the program was written to let the label `F` suggest *finish* and the label `L` suggest *loop*) so that execution escapes the loop `Lbl L .. Goto L` and displays the result of the sum.

In MATLAB

```
% function s = sumN(n)      THM      080709
% (In file sumN.m)
% Sum integers from 1 to n
function s = sumN(n)
s = 0;
for k = 1:n
  s = s + k;
end
```

The nice thing about the MATLAB program is that we can easily change it to sum consecutive triangle numbers instead of just consecutive integers:

```
% function s = sumTriangle(n)      THM      080709
% (In file sumTriangle.m)
% Sum triangle numbers from 1st to nth
function s = sumTriangle(n)
s = 0;
for k = 1:n
  s = s + triangle(k);
end
```

This is called *invoking* the *function* `triangle()` (or "calling" the function). It is very handy to be able to write the code for `triangle` independently and then just use it in another program.

To do this with the TI81 program, we must rewrite `Prgm1:  TRIANGLE` so that it has no input or output (`Input, Disp`) but just accepts and returns values via variables. We cannot use `N`, however, in both `SUMTRIAN` and `TRIANGLE` because we gave different meanings to `N` in the original programs, and they will interfere with each other.

The `sums` programs have a single loop. A program to find the sums of all pairs of squares or cubes has a double loop, one nested inside the other. It also needs a place to store all its results so that they can be displayed. Here is an example calculation, for squares of the first three positive integers, to show what we need.

$j\backslash k$	1	2	3
1	2	5	10
2		8	13
3			18

The storage space needed for up to n squares is clearly the triangular number $n(n+1)/2$, which is 6 in this case for $n = 3$.

The "data structure" provided by programming languages, and some calculators, for such a storage requirement is an *array* or *matrix* of numbers. Such an array might have the name A and hold $n \times n = n^2$ numbers, each "addressed" by values of the *indices* (singular: *index*) j and k, as shown above for 3×3.

Element $j = 2$ and $k = 3$ of A, $A(j,k) = A(2,3)$ is 13 in the above example.

Here is the MATLAB program to calculate the sums of pairs of up to n squares.

```
% function SSD = squareSumDiff(n)      THM      080720
% (Stored in file squareSumDiff.m)
% Generate matrix containing sums and differences of first n squares.
function SSD = squareSumDiff(n)
for j = 1:n
  for k = 1:n
    if j>k SSD(j,k) = j^2 - k^2;
    else   SSD(j,k) = j^2 + k^2;
    end % if j>k
  end % for k = 1:n
end % for j = 1:n
```

(Note that instead of wasting the space below the diagonal of this matrix, which we don't need (why?), the program stores the differences as well as the sums of the squares.)

The TI81 program is limited to 6 × 6 matrices.

```
Prgm4:  SQUARESD
1→J
Lbl A
1→K
Lbl B
if J>K
Goto C
J∧2 + K∧2→[A](J,K)
Goto D
Lbl C
J∧2 − K∧2→[A](J,K)
Lbl D
K + 1→K
If K>6
Goto E
Goto B
Lbl E
J + 1→J
If J>6
Goto F
Goto A
Lbl F
Disp [A]
```

The array name `[A]` is entered by pushing the `2nd` button then the `1` button.

Note the nesting of the loops in both programs, although it is much easier to see in the MATLAB program.

5. Reasoning with rules. Now that we have the idea, from the rules in the first three Notes and from the programs in Note 4, that a letter such as `N` or n can be used simply to stand for any number, we can start doing calculations with letters.

We can only make statements this way that are true for *any* number. So we cannot always say, for instance, $2 \times n = 3$, because that would be true only for a particular *value of* n, i.e., $n = 3/2$.

We *can* always say things such as $2 \times (n + 1) = 2 \times n + 2$ because that is true for every possible number that could be represented by n. (In fact, because there cannot be any confusion, we often omit the × and write just $2(n + 1) = 2n + 1$. We could not do this for numbers only: 2×3 is 6, but 23 is not.)

Let's show that the sum of all positive integers up to n (any number n, but you can start by trying, say $n = 3$ and $n = 4$ to see if it works) is $n(n + 1)/2$. The analog of the visualization in Note 2, in which we combined two triangles to get a rectangle, is to take half of

$$\begin{array}{lllllll} 1 & +\,2 & +\,3 & .. & +\,(n-2) & +\,(n-1) & +\,n \quad + \\ n & +\,(n-1) & +\,(n-2) & .. & +\,3 & +\,2 & +\,1 \end{array}$$

Since $1 + n = 2 + (n - 1) = 3 + (n - 2) = .. = (n - 2) + 3 = (n - 1) + 2 = n + 1$ and since there are n of these sums, all equal, we see that twice the sum from 1 to n is $n(n + 1)$, which is what we hoped to show.

Here is an argument that $n^2 = n + 2\Delta_{n-1}$. Note how it can all be written out in a single chain. It is based on the argument we just made that $\Delta_n = n(n + 1)/2$. Note the modification for Δ_{n-1}.

$$\begin{aligned} n + 2\Delta_{n-1} &= n + 2(n-1)n/2 \\ &= n + (n-1)n \\ &= n + n^2 - n \\ &= n^2 \end{aligned}$$

We can make a similar, if slightly longer, argument about cubes.

$$\begin{aligned} n + 6\Delta_{n-1} + 6\,\diamondplus_{n-2} &= n + 6(n-1)n/2 + 6(n-2)(n-1)n/6 \\ &= n + (3 + n - 2)(n-1)n \\ &= n + (n+1)(n-1)n \\ &= n + (n^2 - 1)n \\ &= n + n^3 - n \\ &= n^3 \end{aligned}$$

We can show that the sum of odd numbers, $2n - 1$ for $n = 1, 2, 3, ..$, is a square number.

$$\begin{aligned} \Sigma(2n-1) &= \Sigma 2n - \Sigma 1 \\ &= 2\Sigma n - \Sigma 1 \\ &= 2\Delta_n - n \\ &= n(n+1) - n \\ &= n^2 \end{aligned}$$

Finally, here is the sum of squares, using $n^2 = n + 2\Delta_{n-1}$ from above.

$$\Sigma n^2 = \Sigma(n + 2\Delta_{n-1})$$

$$
\begin{aligned}
&= \Sigma n + 2\Sigma\Delta_{n-1} \\
&= \Delta_n + 2 \diamondplus_{n-1} \\
&= \frac{n(n-1)}{2} + 2\frac{(n-1)n(n+1)}{6} \\
&= n(n+1)(\frac{1}{2} + \frac{n-1}{3}) \\
&= n(n+1)\frac{3+2n-2}{6} \\
&= n(n+1)(2n+1)/6 \\
&= n(n+1/2)(n+1)/3
\end{aligned}
$$

6. Square roots and cube roots are the ways of going backwards from squares and cubes, respectively.

Thus, since $3^2 = 9$, we use the sign $\sqrt{}$ to go the other way

$$\sqrt{9} = 3$$

Since $2^3 = 8$ (so you see it is very important not the get the order mixed up) we go the other way by a modified $\sqrt{}$ sign

$$\sqrt[3]{8} = 2$$

There are alternative symbols, too. See the table:

n	1	2	3	4	5	6	7	8	..
$n^{\frac{1}{2}}, \sqrt{n}$, sqrt(n)	1	1.4142..	1.7321..	2	2.2361..	2.4495..	2.6458..	2.8284..	
$n^{\frac{1}{3}}, \sqrt[3]{n}$	1	1.2599..	1.4422..	1.5874..	1.7100..	1.8171..	1.9129..	2	

7. Primes. A *prime number* is a positive integer with exactly two different divisors, itself and 1. For example, 2, 3 and 5 are prime. 4 is not (1, 2 and 4 are its divisors). 1 is not (why?).

To check that a number is prime, we could try dividing it by every positive integer smaller than itself.

This would be wasteful in two ways. First, we need not try dividing it by any even number bigger than 2, because if such an even number divides it exactly then so do 2 and whatever times 2 equals the even number, and vice-versa. So we need only try 2 and then odd numbers between 2 and itself.

Second, we don't need to check any potential divisors bigger than the square root of the number, because all bigger integers, if they do go in exactly, will just be the result of dividing by one of the integers smaller than the square root.

For example, for 50, test 2, 3, 5 and 7 only ($7^2 = 49; 8^2, 9^2 > 50$): the test of 2 will reveal 25 as a divisor, so we need not test 25; if we went on to test 5 that would reveal 10 as a divisor so we need not test 10.

Here is a TI81 program which tries 2 then all odd numbers from the integer just below $\sqrt{N}$. (Note that the program starts by making sure N is an integer and at least 2. If not, it stops without producing any result.)

```
Prgm5:  PRIME
Input N
If N ≠ iPart(N)                                    If N is not an integer.
Stop
```

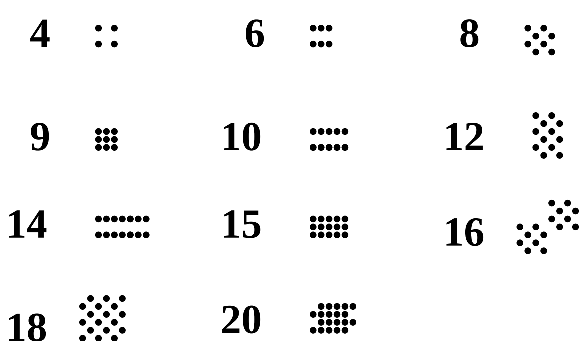
```
If N < 2
Stop
If N = 2
Goto P
If N/2 = iPart(N/2)                      If N is even.
Goto G
iPart( √ (N)) → D                        D is test divisor.
If D/2 = iPart(D/2)
D − 1 → D                                Make D odd.
Lbl L                                    Loop back to here.
If D = 1                                 We haven't found any divisor.
Goto P
N/D → V
If V = iPart(V)                          D divides N exactly.
Goto F
D − 2 → D                                Next smaller odd number.
Goto L                                   Loop back.
Lbl P                                    N is prime.
Disp "PRIME"
Stop
Lbl F                                    N has divisor.
Disp "DIVISOR"
Disp D
Stop
Lbl G
Disp "EVEN"
```

The only new programming operations are √, and `iPart` which gives the integer part (e.g., `iPart(2.1)` is 2, `iPart(2)` is 2, `iPart(−2.2)` is −2).

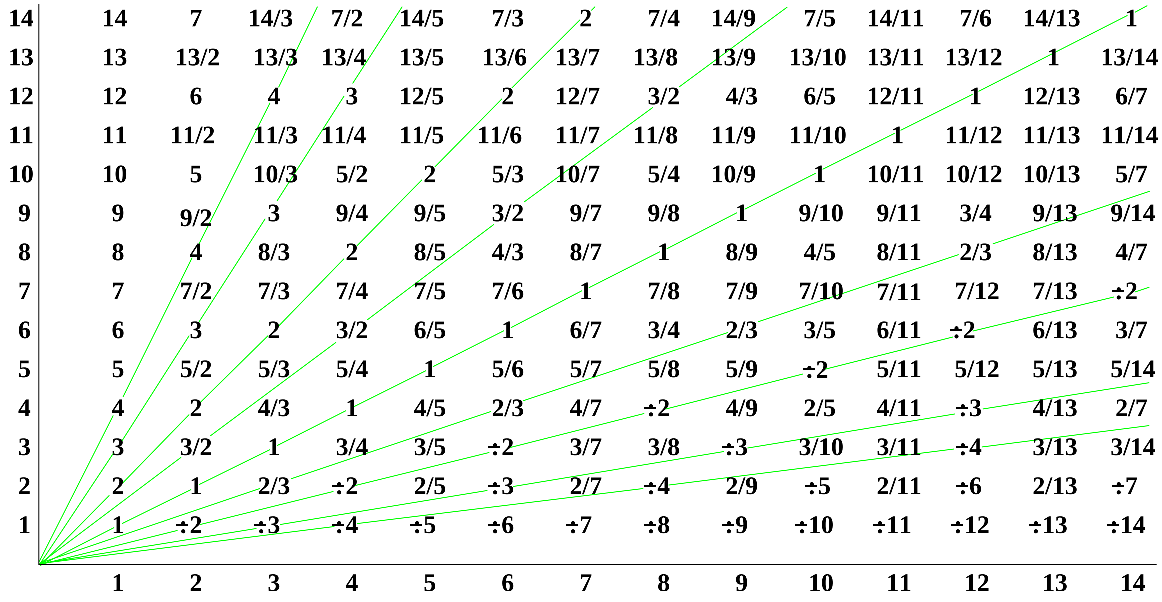
Here is the (much shorter) MATLAB program. In MATLAB, `floor()` does the same for positive integers as `iPart()` does on the TI81. The `mod()` function gives as shorthand way of writing what is in the comment following it.

```
% function p = prime(n)      THM      080709
% (In file prime.m)
% test n for primacy using 2 and odd integers up to sqrt(n)
function p = prime(n)
if n==floor(n) & n>1              % test for plural integer.
  p = true;
  if n~=2
    if mod(n,2) == 0              % if n/2 == floor(n/2)
      p = false;
    else
      for k = 3:2:sqrt(n)
        if mod(n,k) == 0           % if n/k == floor(n/k)
          p = false;
          break
        end % if mod(n,k) == 0
      end % for k = 3:2:sqrt(n)
    end % if mod(n,2) == 0
  end % if n~=2
end % if n==floor(n) and n>1
```

8. Multiplication: rectangles. We can think of multiplication as building “rectangles” in any number of dimensions. Here are some examples.



9. Division: slopes. We can think of division as generating sloping lines. Here are some examples. (The notation ÷2 etc. means 1/2 etc., the *reciprocal*s.)



14	14	7	14/3	7/2	14/5	7/3	2	7/4	14/9	7/5	14/11	7/6	14/13	1
13	13	13/2	13/3	13/4	13/5	13/6	13/7	13/8	13/9	13/10	13/11	13/12	1	13/14
12	12	6	4	3	12/5	2	12/7	3/2	4/3	6/5	12/11	1	12/13	6/7
11	11	11/2	11/3	11/4	11/5	11/6	11/7	11/8	11/9	11/10	1	11/12	11/13	11/14
10	10	5	10/3	5/2	2	5/3	10/7	5/4	10/9	1	10/11	10/12	10/13	5/7
9	9	9/2	3	9/4	9/5	3/2	9/7	9/8	1	9/10	9/11	3/4	9/13	9/14
8	8	4	8/3	2	8/5	4/3	8/7	1	8/9	4/5	8/11	2/3	8/13	4/7
7	7	7/2	7/3	7/4	7/5	7/6	1	7/8	7/9	7/10	7/11	7/12	7/13	÷2
6	6	3	2	3/2	6/5	1	6/7	3/4	2/3	3/5	6/11	÷2	6/13	3/7
5	5	5/2	5/3	5/4	1	5/6	5/7	5/8	5/9	÷2	5/11	5/12	5/13	5/14
4	4	2	4/3	1	4/5	2/3	4/7	÷2	4/9	2/5	4/11	÷3	4/13	2/7
3	3	3/2	1	3/4	3/5	÷2	3/7	3/8	÷3	3/10	3/11	÷4	3/13	3/14
2	2	1	2/3	÷2	2/5	÷3	2/7	÷4	2/9	÷5	2/11	÷6	2/13	÷7
1	1	÷2	÷3	÷4	÷5	÷6	÷7	÷8	÷9	÷10	÷11	÷12	÷13	÷14
	1	2	3	4	5	6	7	8	9	10	11	12	13	14

On the other hand, division is also just multiplying by the reciprocal, so 3/2 is just 3 × (1/2), and we can also imagine this as a 3-by-(1/2) rectangle.

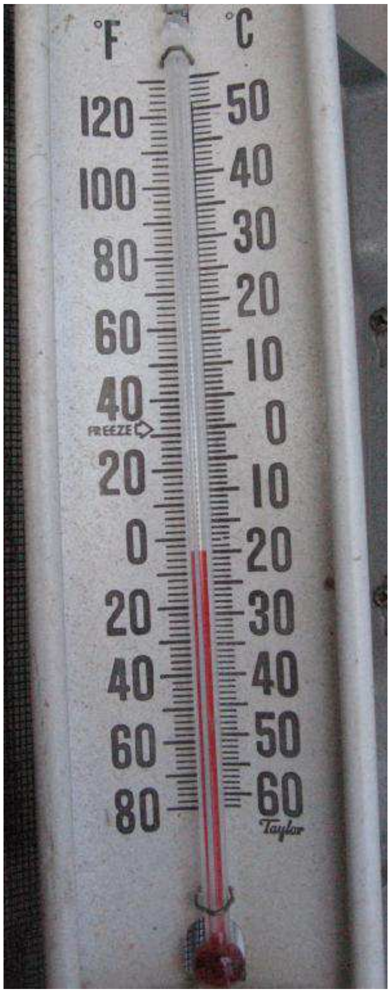
10. Negative numbers. Arithmetic with negative numbers is sometimes difficult. This is not surprising: even the idea of zero needed getting used to and did not enter western mathematics until the Muslim mathematicians passed it on from the Hindu mathematicians.

To make negative arithmetic concrete let's use the example of temperature. We can model the addition operation as a rise in temperature and the subtraction operation as a drop. Temperatures in "temperate" climates such as Canada's often go below 0°C, where they are called "minus", meaning negative, temperatures.

(It is important to distinguish the two uses of the $-$ sign. It can operate on two quantities, as in $3-2$, which is usually prononced "three minus two". Or it can operate on only one quantity, as in -7, which should be pronounced "negative seven". In the temperature example, we'll pronounce $3-2$ as "three drop two" and -7 as "minus seven".)

The arithmetic of $3-2$ is easy: $3-2=1$. It is $2-3$ that is trickier. $2-3=-1$, generally prononced "two minus three equals negative one" but, for temperature, pronounced "two drop three equals minus one".
Temperature make this clearer. If it was 2°C yesterday but dropped by 3C° overnight, it must be -1°C by morning.

Negative numbers make us rethink multiplication, too. For positive numbers we have thought of multiplication as generating rectangles, so 2×3 gives a 2-by-3 rectangle of area 6. When we multiply negative numbers we must take a further step, namely multiplying by -1.



Multiplying by -1 is the operation of *changing direction* on the line of numbers. Thus, on the thermometer, if the temperature has risen 3C°, then changing direction would make it drop 3C°: we say it has risen -3C°.

If we multiply a second time by -1, we change direction again, which on a line can only mean that we are again going in the original direction: $-1 \times -1 = 1$. (Or, being fussy, $(-1) \times (-1) = 1$.)

So multiplying two negative numbers, say

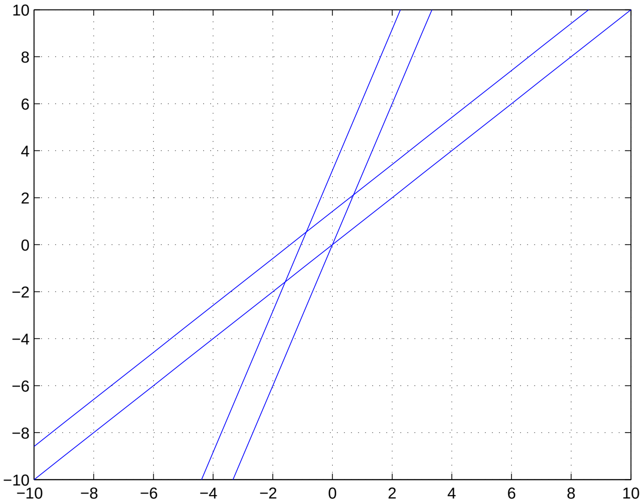
$$-2 \times -3 = (-1 \times 2) \times (-1 \times 3) = -1 \times -1 \times 2 \times 3 = 2 \times 3 = 6$$

requires us to deal with the -1s first, then to think about rectangles.

To multiply a positive by a negative number, take the same steps, but note that the result is negative

$$2 \times -3 = 2 \times (-1 \times 3) = -1 \times 2 \times 3 = -1 \times 6 = -6$$

11. Pictures of rules. Use your calculator or MATLAB to draw the following pairs of "railway tracks".



On the TI81
RANGE button; select Xmin; type (-)10;
(Note that (-), "negative", is different on the calculator from −, "minus". (-)is an "adjective", modifying a single number. − is a "verb", operating between two numbers.)
Still in RANGE:
select Xmax; type 10;
select Xscl; type 1;
select Ymin; type (-)10;
select Ymax; type 10;
select Yscl; type 1;
select Xres; type 1.
Now press the Y= button; select Y$_1$; type X|T;
GRAPH button.

This will plot one of the lines. The other lines may be described under Y$_2$, Y$_3$ and Y$_4$ after pressing Y= again. Let's get this far in MATLAB, too, before thinking about how to get the other lines.

In MATLAB, create a file railwayTracks.m

```
% railwayTracks.m                         THM                               090113
% plot pairs of straight lines: equally separated "railway tracks"
X = -10:1:10;
Y1 = X;
plot(X,Y1,'b')
axis([-10 10 -10 10])
grid on
```

and then type railwayTracks in the command window.

We get the parallel track by adding a "constant" to Y = X. You can try Y$_2$ = X + 1 on the calculator. In MATLAB, this would be Y2 = X + 1 and you must change the plot() line to plot(X,Y1,'b',X,Y2,'b'). Look carefully at the result. It is not what the figure shows. You'll see in a moment that I did not use 1 as the constant.

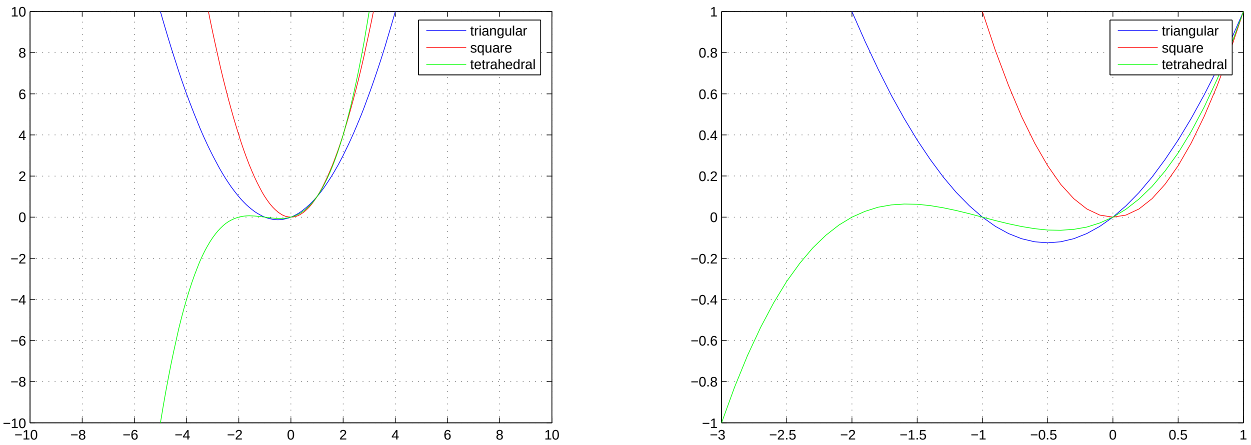
We get a line going in a different direction by multiplying X by a constant. I used Y$_3$ = 3X on the calculator. (Y3 = 3*X in MATLAB and change plot() to plot(X,Y1,'b',X,Y2,'b',X,Y3,'b').)

The multiplier of X is called the "slope" because it gives the direction of the line. For the first two lines, the slope is 1, For the third line it is 3.

The fourth line is another line of slope 3, but moved upwards by adding another constant. Try Y4 = 3*X+1. This is not what I used.

How did I get two pairs of lines separated by equal distances? In fact, if you look closely, those separations are both 1, going perpendicularly from one track to the next in each pair of railway tracks. Try making the constants $\sqrt{s^2+1}$, where s is the slope. That is, $\sqrt{1^2+1}$ for the first pair and $\sqrt{3^2+1}$ for the second.

12. Nonlinear plots. MATLAB and the calculator can also plot the other expressions we have seen this week. Let's try plotting the rule that gives triangular numbers (and the sum of $1+..+n$), $n(n+1)/2$, the rule that gives square numbers, n^2, and the rule that gives tetrahedral numbers (the sum of triangular numbers), $n(n+1)(n+2)/6$.

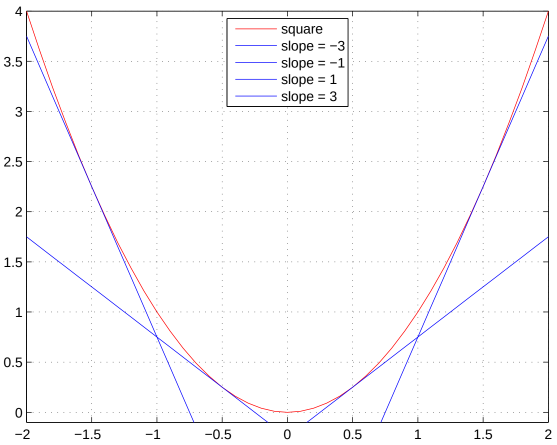


Here is the MATLAB program that gives the zoomed plot on the right.

```
% nonlinPlot.m                          THM                           090113
% plot rules for triangular, square, tetrahedral numbers
X = -3:.1:1;
Y1 = X.*(X+1)/2;
Y2 = X.^2;
Y3 = X.*(X+1).*(X+2)/6;
plot(X,Y1,’b’,X,Y2,’r’,X,Y3,’g’)
axis([-3 1 -1 1])
grid on
legend(’triangular’,’square’,’tetrahedral’)
```

Note that n in the expressions has been renamed X for the program. This is not necessary in MATLAB, but is consistent with the railwayTracks program and with the calculator.

Since the slope of a nonlinear expression in X changes with X, it cannot simply appear as s in the expression itself. Here are a picture of the slopes of X^2 at $X = -3/2, -1/2$, $1/2$ and $3/2$, and the MATLAB program that made the plot.



```
% parabSlope.m       THM        090113
% slope of the rule for square numbers
X = -2:.1:2;
Y1 = X.^2;
Y2 = -3*X - 9/4;
Y3 = -X - 1/4;
Y4 = X - 1/4;
Y5 = 3*X - 9/4;
plot(X,Y1,'r',X,Y2,'b',X,Y3,'b',X,Y4,'b',
     X,Y5,'b')
axis([-2 2 -.1 4])
grid on
legend('square','slope = -3','slope = -1',
 slope = 1','slope = 3','Location', 'Best')
```

13. Summary

(These notes show the trees. Try to see the forest!)

1. Squares and cubes and how to find them using odd and hexagonal numbers or triangle and tetrahedral numbers, and how to sum them using triangle, tetrahedral numbers and the like; pyramidal numbers.

2. Visualizing the relationships among these kinds of number.

3. Programs to calculate some of these kinds of number.

4. Differences of positive integers, their squares and cubes; how far we can go on finding differences.

5. Letters representing any number: the rules for working with letters are the same as the rules of arithmetic.

6. Square roots and distances; cube roots.

7. Prime numbers and programs to test for primacy.

8. Multiplication as rectangle, division as slope.

9. Negative numbers.

10. Plotting: the rules make pictures.

II. The Excursions

You've seen lots of ideas. Now *do* something with them!
(Some excursions are credited to the people who are not necessarily their originators but who suggested them to me.)

1. **Mathematical truth** Does 1 + 1 always = 2? Think about a drop of rain on the car window (1) encountering a nearby raindrop (+ 1): do they remain 2 raindrops or become 1 (1 + 1 = 1)? Think about lending a friend your pet female rabbit (1) while your family goes away on an assignment for a year or two, and your friend already has a pet male rabbit (+ 1): are you sure there will be exactly 2 rabbits when you return, or does, maybe, 1 + 1 = 7 in this case?
Mathematical truths are different from scientific truths. If a counterexample is found for a

scientific statement (such as "the sun rises every morning (in Montreal)"), that statement is not a scientific truth. Mathematical statements are abstractions from important situations (most of the times we can think of, $1 + 1 = 2$) and it is being useful that makes them important: they help us reason in the situations where they do apply, or they give us useful ideas to understand such relevant situations.
Think of some situations where counting and adding are useful, and of some situations where they are not.

2. **Counting in tongues.** Find out how to count from 0 to a million-1 in as many different languages as possible. How many different words does each language need to do this? Which language has the fewest different words? How many more words does it take to count from a thousand to a million-1? From a hundred to a thousand-1? (Travellers' phrase books are usually easier to use for this research than translation dictionaries.)

3. How does $2n-1$ reveal that it describes all the odd numbers? Hint; What describes the even numbers? If you ask me to get at least five apples and offer to repay me 2$ per apple, you know you will be paying me at least 10$. If I buy an extra apple, how much more must you pay?

4. In the representation of odd numbers in Note 1, how many asterisks are there per side of each diagram? How would I get $2n-1$ out of this?

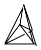
5. 1 2 3 4 5 6 7 8 9 10 = 100
   Find a way to replace some of the blanks by + so that the above is true. If a blank is not replaced by + then the digits either side of it are combined to form a multi-digit number, e.g., 1 + 2 + 3 = 6,   1 2 + 3 = 12 + 3 = 15,   1 + 2 3 = 1 + 23 = 24,   1 2 3 = 123.
   Can you do it with only the nine digits 1 .. 9 = 100? What if you use other operators as well as +: $-$, $\times$, $\div$?

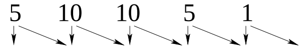
6. **Squares.** Find pairs of square numbers which:
   a) sum to another square (Find three examples and say which can be calculated from which others. Such sets are called *Pythagorean triples.* Look up Pythagoras of Samos 580–572 BCE to 500–490 BCE);
   b) sum to a prime number (A *prime* is a positive integer which has exactly two different divisors, itself and 1. Why is 1 not a prime under this definition?);
   c) sum to a number, not necessarily square or prime, which is also the sum of two other squares.
   d) Find a number whose square and cube sum to the square of twice itself ($n^2 + n^3 = (2n)^2$ Try $(2n)^2 - n^2 = n^3$).

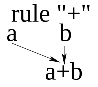
7. **Cubes.** Find pairs of cubic numbers which:
   a) sum to a prime number (Think laterally!);
   b) sum to a number which is also the sum of two other cubes (The smallest such is called Ramanujan's number: look up Srinivasan Raman*u*jan, 1887–1920.).
   c) A *Fermat triple* is three numbers, k, m, n, such that $k^p + n^p = m^p$ for any integer $p > 2$. Can you find any for $p = 3$? Look up Pierre Fermat (1601–1665) and "Fermat's Last Theorem".
   d) Find three adjacent positive integers whose cubes sum to the cube of the next integer.
   e) Show that 1, 3+5, 7+9+11, 13+15+17+19, 21+23+25+27+29 and so on are cubes. Use results in the sum table and the difference table to argue that this is generally true. (Note the average value and the number of entries in each of these groups.)

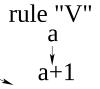
8. **Simplex numbers.** Instead of thinking about simplices as piles of asterisks (or blocks or balls), let's think of them as stick figures. Then we can distinguish *vertices, edges, faces, solids,* and so on, which we can abbreviate V, E, F, S, etc., respectively. (A "vertex" means

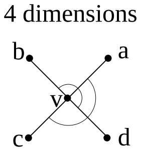
a point or a corner, an “edge” is a single straight-line segment, a “face” is a single flat 2-dimensional facet, a “solid” is a 3-dimensional volume.)
Here are pictures and numbers for 2, 3 and 4 dimensions.

d		V	E	F	S	...
0						
1						
2		3	3	1		
3		4	6	4	1	
4		5	10	10	5	1
5						



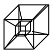


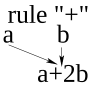


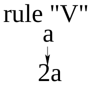


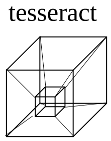
a) Check that the numbers are right. You may have a little difficulty seeing that there are 10 faces and 5 solids in four dimensions. Use the diagram on the right, which shows the one vertex, v, that has been added to the 3-D simplex (tetrahedron) to turn it into a 4-D simplex, and which shows the four vertices that were already present in the tetrahedron, a, b, c and d. In addition to the 6 triangular faces already in the tetrahedron, there will be 6 more: use v and the existing 6 edges from the tetrahedron *ab, bc, cd, da* and *ac* and *bd.* These last two are shown as little arcs.
Use the same diagram to imagine 4 new solids in addition to the 3-D tetrahedron *abcd*: a new tetrahedron can be constructed by replacing each of a, b, c and d in turn bt the new vertex v.
b) Check that the two rules are right. What is the *reason* the vertex counts go up by 1 each time we add a dimension? What is the *reason* we add, say, the numbers of edges and faces from the previous row to get the number of faces for the current row?
c) What will the next row be (5 dimensions)? And the next? Now you’re thinking in any number of dimensions.
d) What about 1 dimension and 0 dimensions? Can you apply the rules backwards and draw the corresponding figures?
e) Look for a line (not necessarily horizontal or vertical) of numbers in the table which gives the triangular numbers, and for a line giving the tetrahedral numbers.

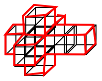
9. **Hypercube numbers.** Similarly, let’s think of squares, cubes, etc. as stick figures and count vertices, edges, faces, solids, etc. for these, as in the previous Excursion.

d		V	E	F	S	...
0						
1						
2		4	4	1		
3		8	12	6	1	
4		16	32	24	8	1
5						









a) Check the numbers. Again, 4 dimensions might appear to be a barrier, so the diagram on the right is an expansion of the picture in the table for the “tesseract”, which is the name of a 4-hypercube (a 4-dimensional cube). It is two cubes, one shown inside the other, with all 8 corresponding pairs of vertices connected.
(Also shown, below the tesseract, is another way of imagining this 4-dimensional figure: think of what a square would look like laid out on a piece of cardboard ready to be cut out and

folded; then extend this thinking to a bunch of connected cubes in 3-D instead of connected squares in 2-D. The black shows the complete cubes; the red shows the outline. Count the number of cubes. Imagine which edges and faces must coincide when it is all "folded" up and count all distinct edges and faces to check the table.)
b) Check the rules: why do the vertices double and why is there a factor of 2 in the $a + 2b$?
c) What are the numbers in the row for 5 dimensions? 6 dimensions?
d) What are the numbers and the diagrams in the rows for 1 dimension and 0 dimensions?

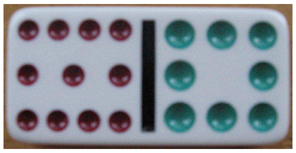
10. Write n^2 as the sum of two triangles of different sizes and nothing else.

11. Write n^3 as the sum of six tetrahedra of different sizes and nothing else.

12. How would you stack ten ears of sweet corn on a dish?

13. (Ken Murata) How would you display ten nectarines for a party?

14. How many different dominos are there? Each represents a pair of numbers from 0 (blank) to 12. There are no duplicate dominos. The two numbers may be the same. Here is (8,11)—which is the same as (11,8).



15. The connection between powers and triangle numbers, tetrahedral numbers and so on is given by *Stirling numbers*, which take relationships such as

$$n^2 = n + 2\Delta_{n-1}$$

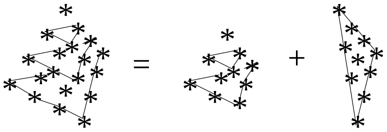
and

$$n^3 = n + 6\Delta_{n-1} + 6\,\diamondplus_{n-2}$$

to any number of dimensions. Look up Stirling numbers.

16. Find a way to write the nth pyramidal number as two tetrahedral numbers, and a way to write the nth square number as three pyramidal numbers.

17. Supposing that $\diamondplus_n = n(n+1)(n+2)/6$, show that $\diamondplus_{n+1}$ has the corresponding form $(n+1)((n+1)+1)((n+1)+2)/6$.



18. Compare the constants we got at the end of the differencing processes for n^2 and n^3 with the denominators of the formulas giving the triangular numbers and the tetrahedral numbers, respectively.

19. Show that the sum of the reciprocals of *all* the triangular numbers is 2. (Hint: $1/(n(n+1)) = 1/n - 1/(n+1)$.) What is the sum of the reciprocals of all the tetrahedral numbers?

20. What does the following series sum to?

$$\frac{1}{(\sqrt{2}+\sqrt{3})} + \frac{1}{(\sqrt{3}+\sqrt{4})} + .. + \frac{1}{(\sqrt{99}+\sqrt{100})}$$

21. Show that $(\Delta_d)^2 - d\,\diamondplus_d = d^2(d^2-1)/12 = \Delta_{\Delta_{d-1}} - S^4_{d-3}$, where S^4_n is the nth 4-dimensional simplex (see Excursion *Simplex numbers*), $S^4_n = n(n+1)(n+2)(n+3)/24$. These complicated expressions are interesting because they each give the number of ways a d-dimensional space can curve. To find out what this means you must carry on to Book 11c, on general relativity.

22. Rewrite the TI81 `Prgm1: TRIANGLE` and invoke it from `Prgm3: SUMN` modified to sum triangle numbers instead of integers.

23. **Simplexes: higher-dimensional triangles.** A *simplex* is a generalization of the triangle: a triangle is a "2-simplex", i.e., a simplex in two dimensions. Let's count components, or "parts of space", in the 2-simplex: it has 3 *vertices* or corners; it has 3 edges; and it has one *face*, i.e., the triangle itself.

   A 3-simplex is a tetrahedron, formed by adding one vertex, in a third dimension, to the 2-simplex. It has, of course, 4 vertices; it has 6 edges—the three of the triangle plus three more connecting the new vertex to each of the three old ones; it has 4 faces (hence the "tetra" in "tetrahedron": "$\epsilon\delta\rho\omega\nu$" means "base" in Greek—or "seat", except on busses where they are "$\theta\epsilon\sigma\epsilon\sigma$"—and mathematics has extended it to mean "face"); and finally it has one other component, itself, for which we have no category name in English.

   We can back down to one dimension: remove a vertex from a triangle to get a 1-simplex, which has 2 vertices, 1 edge, and no higher-dimensional parts of space.

   Backing all the way down to zero dimensions, a 0-simplex is a single point, i.e., 1 vertex and no more.

   a) Now confirm the following table for simplexes of up to seven dimensions. (You'll need to look for patterns in the numbers: nobody can visualize a simplex in that many dimensions. What is the rule for getting the next row?)

d Dimensions	d-simplex	v vertices	e edges	f faces					
0	point	1							
1	line	2	1						
2	triangle	3	3	1					
3	tetrahedron	4	6	4	1				
4		5	10	10	5	1			
5		6	15	20	15	6	1		
6		7	21	35	35	21	7	1	
7		8	28	56	70	56	28	8	1

   Find a pattern of numbers very similar to this in Week_ii. b) Build a model tetrahedron, say out of pipe cleaners. What must you add to it to build a 4-simplex?

24. **Hypercubes: higher-dimensional squares.** a) By thinking in the same way as for the previous Excursion, you can confirm the following table for the generalizations of squares to any number of dimensions. What is the rule for getting the next row this time?

d Dimensions	d-hypercube	v vertices	e edges	f faces					
0	point	1							
1	line	2	1						
2	square	4	4	1					
3	cube	8	12	6	1				
4	tesseract	16	32	24	8	1			
5		32	80	80	40	10	1		
6		64	192	240	160	80	12	1	
7		128	446	572	560	320	104	14	1

   b) Build a model cube out of pipe cleaners. What must you add to it to build a tesseract? Also build a model cube out of cardboard by cutting out and folding up a single shape. Using the numbers in the table for the tesseract can you draw the 3-dimensional shape that would have to be "folded up" to make a tesseract?

25. **Hyperdipyramids: higher-dimensional squares, part 2.** An *octahedron* is a "dipyramid": two pyramids based on a square, with one apex above and one below the square. It can also be thought of as having vertices at $(\pm 1, 0, 0), (0, \pm 1, 0)$ and $(0, 0, \pm 1)$ in a 3-dimensional coordinate system. The 4-dimensional generalization adds two more points and connects each to each vertex of the octahedron. It also doubles the number of parts of space one dimension down: the octahedron has 8 triangular faces, the 4-dipyramid has 16 tetrahedral components.
a) Confirm the following table for dimensions 1 to 7.

d Dimensions	d-dipyramid	v vertices	e edges	f faces					
0	point	1							
1	line	2	1						
2	square	4	4	1					
3	octahedron	6	12	8	1				
4		8	24	32	16	1			
5		10	40	80	80	32	1		
6		12	80	160	240	192	64	1	
7		14	104	320	560	572	446	128	1

b) What is the relationship between hyperdipyramids and hypercubes? Each is the "dual" of the other: what does this mean?
c) The suffix "gon" (Greek $\gamma\omega\nu\iota\alpha$ angle) is used for 2-dimensional figures, "hedron" (Greek $\epsilon\delta\rho\omega\nu$ base) is used for 3-dimensional figures, and "tope" (Greek $\tau\omega\pi\omega\sigma$ place) is used for figures of any dimensionality, including 2 and 3, but usually restricted to dimensions 4 and up. The prefix usually counts, in Latin, the number of components whose dimension is one less than the dimensionality of the full figure. Thus, a square is a quadragon, a cube is a hexahedron, a 4-simplex is a pentatope, a tesseract is an octatope, and a 4-dipyramid is a hexadecatope.
Coexeter [Cox63] says that only simplexes, hypercubes and hyperdipyramids exist as *regular* figures in arbitrarily high dimensions. (A regular figure has all sides the same length, all faces, if applicable, the same size, and so on.) How many different regular figures are there in two dimensions? Three dimensions? Four? Five?

26. "Martian arithmetic" (Eugene Lehman.) Martian arithmetic uses $+$, $-$, $\times$, $/$ and $^\wedge$ in the proper way, but scrambles the meanings of the ten digits 0,1,2,3,4,5,6,7,8,9. The Marinaris Stone, discovered on the Moon and identified as an ejectum from a Martian asteroid strike, contains the only clues:
a) $8\times 7 = 8$
e) $7^\wedge 4 = 6$
c) $7 - 33 = -1$
b) $4\times 9 = 39$
d) $51/2 = 2$
f) $3+65 = 69$
What are ? (in Martian **and** Earthian) in
h) $7+? = 9$
g) $40+94 = ?$

27. Choose two specific successive values of n to work through the argument in Note 5 about the sum of the first n positive integers. (For instance, 100 and 101.)

28. For each step in the arguments in Note 5, explain which property of arithmetic on "any number n" allows the step to be made.

29. (Via Alan Malkin.) Here are two 3-triangles filled with integers from 1 to $\Delta_3 = 6$. Note that all three sides of each triangle sum to the same total, 9 in one case, 12 in the other. How many other sums can you find, and what are the corresponding 3-triangles?

1
6 5
2 4 3
	6
	2 1
	4 3 5

30. (Eugene Lehman.) Eugene usually takes the 17:00 train home after a day of teaching unnecessarily advanced mathematics in the school, but last week a class was cancelled and he took the 16:00 train. Shirley always drives to the station arriving just in time to meet the 17:00 train. Since she was not there yet when Eugene arrived on the 16:00 train last week, he started walking along her route. When they met she picked him up and took him straight home, arriving there half an hour earlier than usual. How long did Eugene walk?
Use letters, t for the usual arrival of the 17:00 train, d for Shirley's usual *round-trip* drive, variants t' and d' for the corresponding times and durations last week, and w for how long Eugene walked last week, make an equation relating the usual commute with last week's, and see what arithmetic on the letters tells you.

31. (Eugene Lehman.) The bank teller made a mistake and instead of withdrawing and giving you D dollars and C cents, which you asked for, gave you instead C dollars and D cents. You had spent 5 cents in a chewing gum machine before you counted up and found you now had exactly twice what you had asked for. How much was that?
a) Show that $98C - 5 = 199D$. The process of arriving at this equation from the equation you should start with is called "The Balance", or, to the Arabs who invented it, "al jabr": if you add anything on one side of the "=" you must also add it on the other side, or else the equation will get out of balance; if you subtract anything from one side of the "=" you must also subtract it from the other. This is true whether you are doing arithmetic on letters or just on numbers.
b) (a) gave you one equation in two unknowns. Think of a second equation in C and D which is approximately true, from the statement of the problem, and see what the two equations give you. You may have to modify your approximation, but after just a little trial and error you should find a solution.
c) Write a calculator program instead of (b), which takes, say, C through all possible values (what are they?) and uses (a) to find, say, D for each one. It can stop the first time you find a D which is an integer (whole number).
d) Integer problems such as this are called Diophantine. Look up Diophantus ($\sim$ 200–$\sim$ 284).

32. (Wofgang Rasmussen.) A jug contains exactly one litre of white wine. A second jug contains exactly one litre of red wine.
a) Suppose you take a ladleful of white wine from the first jug and pour it into the second. Then take exactly the same amount of the mixture from the second jug and pour it back into the first. Show that, after this, the amount of red wine in the first equals the amount of white wine in the second. Hint: let W litres be the amount of white now in the second jug. How much red is in the second jug? How much white is in the first jug? How much red is in the first jug?
b) What if you had used a teaspoon instead of a ladle? A half-litre cup? The whole litre? What if you had done several transfers (an even number) with exactly the same amounts going each way?
c) Another way to look at (a) is to show, assuming red and white molecules are the same size, that the number of molecules of red in the ladle going from jug 2 back to jug 1 is the same as the number of molecules of white left in jug 2 after the mixture has been transferred to jug 1. Hint: let m be the number of molecules in a ladleful and w be the number of white molecules left in jug 2 at the end.
d) You are led to a table in a darkened room, on which you are told that there are a couple of decks of cards, all face-down except for 10 that have been turned face-up. You are instructed

to make a second pile from among the cards in that pile, such that the number of face-up cards is exactly the same in the two piles, old and new. You are allowed to do anything you like with the cards, but not damage them or turn on a light. How do you do it?

33. (Ramanujan's address.) Ramanujan lived at address R on a one-sided street of N houses (houses are numbered consecutively from 1 to N, including R); he could never remember his own address (unlikely for Ramanujan, who was friends with every number) but he could remember that the sum of the addresses below but not including his equalled the sum of the addresses above but not including his; how many houses were on the street and where did he live?
a) Why does this problem involve finding triangular numbers which are also square numbers? Try writing three columns, n, Δ_n and $\Box_n$, and rows for $n = 1..10$ or 12. Can you find two solutions among these numbers?
b) Can you think of a shortcut? Why must either both $N/2$ and $N+1$ or both N and $(N+1)/2$ be squares?
c) If Ramanujan's street contains between 50 and 500 houses how long is it and where does he live?
d) Write a program to find subsequent pairs (R, N). Look for patterns in the results.

34. Check the roots of Note 6 and confirm in particular that $(\sqrt{n})^2 = n$ and $(\sqrt[3]{n})^3 = n$.

35. What are $\sqrt{3^2+4^2}$, $\sqrt{5^2+12^2}$, $\sqrt{9^2+12^2}$, $\sqrt{8^2+15^2}$, $\sqrt{6^2+8^2}$?

36. On a new sheet of paper (which will have right angles at each corner) carefully measure 4cm down from the top left corner and 3cm rightwards from the same corner. Carefully measure the length of the line connecting the two points you marked at the edges.
Measure 5cm rightwards from the bottom left corner and 12cm upwards. How long is the connecting line?
Measure 12cm leftwards from the bottom right corner and 9 cm upwards, and complete and measure the triangle. Measure 8cm left and 15cm down from the top right corner.
Cut out the four triangles you have just drawn and see what kinds of patterns you can make with them. Make extra copies of the triangles and more patterns. Find a fifth triangle with the same property you noticed in the first four and make still more patterns.

37. What is the pattern that finds Pythagorean triples which include two adjacent integers?

38. a) Explore the sequence

$$\frac{1}{1}, \frac{3}{2}, \frac{7}{5}, \frac{17}{12}, ..$$

in which each fraction is made from the preceding fraction $\frac{n}{d}$ by the rule

$$\frac{n}{d} \to \frac{n+2d}{n+d}$$

starting with $\frac{1}{1}$.
Look for a pattern in the sequence of squares of these fractions.
b) Explore the sequence made by the rule

$$\frac{n}{d} \to \frac{n^2+2d^2}{2nd}$$

starting with $\frac{1}{1}$.
Is there any overlap with the previous sequence?
c) Now try

$$\frac{n}{d} \to \frac{n+sd}{n+d}$$

for any given number s, say $s = 2$, $s = 3$, $s = 3/2$, .. Compare these new sequences with

$$\frac{n}{d} \rightarrow \frac{n^2 + sd^2}{2nd}$$

for the corresponding s.

39. Find the twenty-five prime numbers less than 100. Hint: it is fastest to eliminate as many non-primes (*composites*) as possible, instead of checking many numbers for being prime, even if you have available the prime-finding programs. Write down 2 and odd numbers > 1 unless they are divisible by 3, by 5 or by 7.
(Numbers are divisible by 3 if the sum of their digits is divisible by 3: e.g., the number 1023. Numbers are divisible by 5 if the last digit is 0 or 5, and 0 will not happen for odd numbers. All that is left is to check divisibility by 7.)
Why do we not need to go beyond 7?

40. The *Sieve of Eratosthenes* is a more sophisticated method to test if a positive integer is prime. Instead of checking 2 and all odd numbers above 2 as divisors, the "sieve" checks only primes up to the square root of the number. (The first argument in Note 7 applies not only to even divisors but to all composite divisors.)
a) Look up the Sieve of Eratosthenes ($\mathrm{E}\rho\alpha\tau o\sigma\theta\epsilon\nu\eta\varsigma$, Eratosthenes of Cyrene, 276–195 BCE). To program this you will need a table of prime numbers, which you add to every time you discover a new prime. Think about how you would use an array to do this.
b) Leonhard Paul Euler (1707–83) discovered (or invented) an application of the Sieve which converts an infinite sum over all numbers into an infinite product over all primes. Show that the "harmonic series"

$$\zeta = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} + \frac{1}{10} + \frac{1}{11} + \frac{1}{12} + \frac{1}{13} + ..$$

satisfies

$$(1 - \frac{1}{2})\zeta = 1 + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{9} + \frac{1}{11} + \frac{1}{13} + ..$$

and then

$$(1 - \frac{1}{3})(1 - \frac{1}{2})\zeta = 1 + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + ..$$

and

$$(1 - \frac{1}{5})(1 - \frac{1}{3})(1 - \frac{1}{2})\zeta = 1 + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + ..$$

So, eventually,

$$\zeta = 1/\Pi_p(1 - \frac{1}{p})$$

where Π_p means take the product over all primes, p.
(Actually the harmonic series becomes arbitrarily large, and Euler's "product formula" is more interesting for the generalization

$$\begin{aligned}\zeta(s) &= 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \frac{1}{6^s} + \frac{1}{7^s} + \frac{1}{8^s} + \frac{1}{9^s} + .. \\ &= 1/((1 - \frac{1}{2^s})(1 - \frac{1}{3^s})(1 - \frac{1}{5^s})(1 - \frac{1}{7^s})..)\end{aligned}$$

which does have a finite value for every $s \neq 1$. Georg Friedrich Bernhard Riemann's (1826–66) "zeta function" $\zeta(s)$ is thoroughly chronicled by [Der03], who discusses its relationship with the primes: knowing the zeros of the zeta function will tell us how the primes are

distributed—not the zeros at every even negative integer value of s but those in the 2-number plane off the 1-number line.)
c) How do we know that there are infinitely many primes? $E\upsilon\kappa\lambda\epsilon\iota\delta\eta\varsigma$, Euclid of Alexandria ~300 BCE, argued that if N is the last prime then $2 \times 3 \times 5 \times .. \times N - 1$ is either prime or has a prime factor larger than N, so there can be no last prime in either case.

41. **Rectangular numbers: multiplication** a) Make "rectangles" in two or three or more dimensions in as many different ways as you can for as many different integers as you like, building on the table in Note 8. For each "rectangle" write in numbers the multiplication it represents.
b) Use the two-dimensional rectangular numbers to show that multiplication is *commutative*

$$a \times b = b \times a$$

Use the three-dimensional rectangular numbers to show that multiplication is *associative*

$$(a \times b) \times c = a \times (b \times c)$$

What other arithmetic operations are commutative and associative?

42. (Eugene Lehman: How much is your name worth?)
a) Calculate the value of your name by multiplying the letters coded `a` = 1\$, `b` = 2\$, .., `z` = 26\$. For example, `Eugene` = $5 \times 21 \times 7 \times 5 \times 14 \times 5\$ = 2 \times 3 \times 5^2 \times 7^3\$ = 51450\$$; `Lehman` = $12 \times 5 \times 8 \times 13 \times 1 \times 14\$ = 2^6 \times 3 \times 5 \times 7 \times 13\$ = 87360\$$
b) Now find a word or short phrase that will sell for exactly a million dollars. (Hint: which letters are divisors of 1 000 000?)

43. (Eugene Lehman) Two of the guests at a birthday party turn out to have the same birthday as the celebrant, even though all three are not necessarily the sme age. Figure out all their ages from the following facts.
i) The three ages multiply to 36.
ii) The three ages sum to the number of people at the party.
iii) The eldest of the three is from the U.S.
Also say why (iii) is needed.

44. **Al jabr** The Arabic term for "the balance" describes the process of keeping equations balanced: we can do any arithmetic operation on one side of the equation and as long as we match it with the same operation on the other, the two sides are still equal.
a) Suppose we happen to know that $\phi = 1 + 1/\phi$. How can we find out that $\phi^2 - \phi - 1 = 0$ by (i) multiplying both sides by the same thing and (ii) subtracting the same thing from both sides?
b) *Diophantine* equations are restricted to integer solutions. Al jabr applies for addition, subtraction and multiplication but not always for division. Inspect Eugene's bank teller excursion, above, from this point of view.
c) **The mystery of cancellation.** *Al jabr* also applies to fractions, in an even more limited way. Only multiplication and division can be done to both the numerator and the denominator if we want to reach a fraction having the same value. Thus in Note 10, 8/12 is shown as 2/3 because we can divide both the top and the bottom by 4.
But if we *add* the same number to both numerator and denominator we do not get a fraction having the same value: try adding 3 to both top and bottom of 1/2.

45. **Slopes: division** a) Extend the division diagram in Note 9 to as many divisions as you like. Explain the appearance of more than one fraction on some of the lines. In the full diagram, which would go on forever upwards and rightwards, what would be the smallest number of fractions on any one line?

b) Figure out the following diagram and add some more fractions in their approximate positions on the horizontal line of numbers from 0 to 1.

$$\mathbf{0} \quad \frac{1}{9}\frac{1}{8}\frac{1}{7}\ \frac{1}{6}\ \ \frac{1}{5}\frac{2}{9}\ \frac{1}{4}\ \ \frac{2}{7}\ \ \frac{1}{3}\ \ \frac{3}{8}\ \frac{2}{5}\ \frac{3}{7}\frac{4}{9}\ \ \ \frac{1}{2}\ \ \ \frac{5}{9}\frac{4}{7}\ \frac{3}{5}\ \frac{5}{8}\ \ \frac{2}{3}\ \ \frac{5}{7}\ \ \frac{3}{4}\ \frac{7}{9}\ \frac{4}{5}\ \ \frac{5}{6}\ \frac{6}{7}\frac{7}{8}\frac{8}{9} \quad \mathbf{1} \quad \frac{9}{8}\frac{8}{7}\ \frac{7}{6}\ \ \frac{6}{5}\ \ \frac{5}{4}\ \frac{9}{7}\ \ \frac{4}{3}\ \frac{10}{8}\frac{7}{5}\frac{10}{7}\ \ \ \frac{3}{2}$$

1/3 = 2/6 < 3/6 = 1/2

3/7 = 27/63 < 28/63 = 4/9

n/d < m/c or n/d = m/c or n/d > m/c

n/d ≤ m/c or n/d > m/c

n/d ≤ m/c or n/d ≰ m/c

if a ≤ b and b ≤ c then a ≤ c

if a ≤ b and b ≤ a then a = b

if a = b then a ≤ b and b ≤ a

a ≤ b and b ≤ a iff a = b

c) *Al jabr* works for inequalities as well as equalities. Just above we see that $3/7 < 4/9$ because we can multiply top and bottom of the first by 9, to give a fraction of the same value, and we can multiply top and bottom of the second by 7, to give a fraction of the same value as 4/9. Since 27<28, so 27/63<28/63.
Show that if $\frac{n_1}{d_1} \leq \frac{n_2}{d2}$ then

$$\frac{n_1}{d_1} \leq \frac{n_1+n_2}{d_1+d_2} \leq \frac{n_2}{d2}$$

d) Show that division is *palindromic*

$$\begin{aligned} a &= b/c \\ &\Updownarrow \\ c &= b/a \end{aligned}$$

What other arithmetic operations are palindromic?
e) **Approximate arithmetic** An example of division is speed

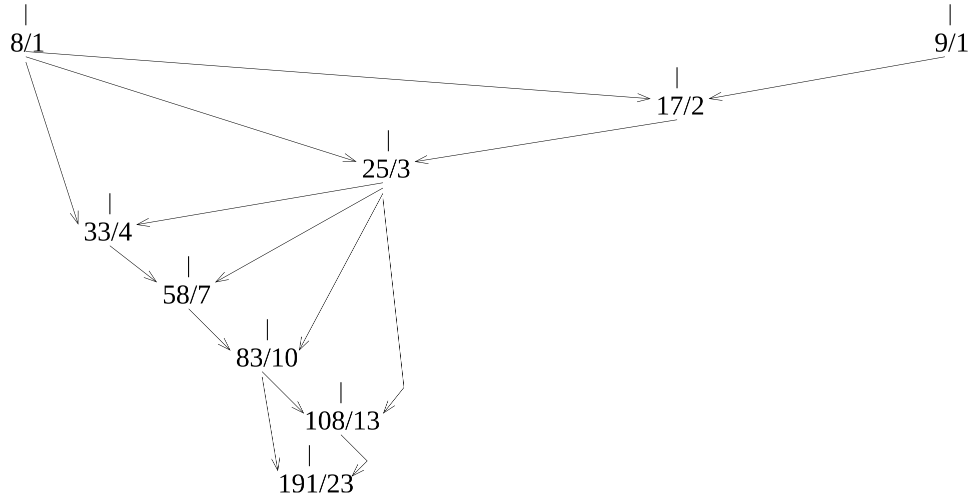
$$s = d/t$$

The speed s is the distance d travelled divided by the time t taken.
Palindromically we can calculate how long it will take to make a trip if we know the distance and the speed (or, at least, the average speed)

$$t = d/s$$

If we are driving 100Km on a quiet highway at the speed limit of 100Km/hour, we know it will take us an hour. But if the highway gets busy and we are only making 90Km/hour we can calculate 100Km/(90Km/hour) = 1.11 hours or about 67 minutes.
However it is not legal in many jursidictions to use a calculator or a pencil and paper while driving, even at 10Km/hour under the speed limit. Nor is it safe, especially on a busy highway. So we would like to do this kind of calculation in our head.
Here is an approximation. Since we are driving 10% slower than the speed that would get us there in an hour, it should take us 10% longer than the 60 minutes, i.e., 66 minutes.
This is pretty close. If we were driving 50% slower, though, the time would be double, not just 50% longer.
Make a table of speeds, both under and over 100Km/hour by 1%, 2%, 5%, 10% 20% and 50%, and put into it the exact and the approximate calulations of how many minutes the trip will take. When is the approximation close enough to make no difference to the nearest minute?
(By the way, how much time do you actually save by driving 100Km at 20% over the speed limit? Since it will cost you more than 20% more fuel, and possibly a heavy fine to boot, is it worth it?)

46. (Brocot fractional approximation) The Brocot algorithm [Hay08, Ch.7] finds fractional approximations to given numbers, motivated by the mid-19th century need to design gear ratios. Here it finds successive approximations to 191/23, starting at the underestimate 8/1 and the overestimate 9/1. 17/2 = (8+9)/(1+1) will be closer than either because it averages both numerator and denominator. 9/1 had a larger error than 8/1, so it gets replaced and the next "average" is of 8/1 and 17/2: 25/3. Eventually we get the exact answer, 191/23, since this was itself a fraction all along. But we see that 108/13 and 83/10 are approximations to it, if we could not make a gear with 191 teeth, for example.



The diagram shows the successive approximations positioned to the left and to the right of 191/23 according to their error. Be careful: this error is not measured $G - N/D$, where the goal G is the number sought (191/23 in this case) and N and D are the numerator and denominator, respectively, of the approximation. Rather, the "error" is $GD - N$, otherwise the algorithm does not give the final 191/23. (The final result also depends on the choice of the initial straddling approximations, in this case 8/1 and 9/1.)
Write a program for your calculator or in MATLAB to implement Brocot's algorithm. Let it input both the number to be approximated and the tolerance acceptable, and read the initial straddling approximations from an array of twice three elements: the numerator, the denominator, and the error which your program will calculate at each step. Replace the old approximation that has the greater "error" $GD - N$ by the "averaged" approximation.
The tolerance should be compared with the true error, $G - N/D$.
Experiment with your program. For instance 191 and 0 can be input as goal and tolerance, and the array [8,1,0;9,1,0] as the straddling approximations. Or π and 0.01, straddled by [3,1,0;4,1,0], gives the sequence of fractions 3/1, 4/1, 7/2, 10/3, 13/4, 16/5, 19/6 and 22/7, the last being the classical schoolchild approximation to π. Or $(1+\sqrt{5})/2$ and 0.001, straddled by 1/1 and 2/1, gives the first dozen terms of the Fibonacci sequence (Week ii Note 2).

47. Better than Brocot: **continued fractions.** A continued fraction has the form

$$a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \cdots}}}$$

which may stop at a certain level or may go on forever. If it represents a rational number (e.g., a fraction) it will stop.
a) Here's how to work out 191/23, the fraction in the Brocot Excursion.

f	$\lfloor f \rfloor$	fracpart(f)
$\frac{191}{23}$	8	$\frac{7}{23}$
$\frac{23}{7}$	3	$\frac{2}{7}$
$\frac{7}{2}$	3	$\frac{1}{2}$
2	2	0

Here $\lfloor\frac{191}{23}\rfloor = 8$, meaning find the largest integer less than the fraction. And fracpart$(\frac{191}{23}) = \frac{191}{23} - \lfloor\frac{191}{23}\rfloor = \frac{7}{23}$, meaning find the fractional part.
Note that f beginning each line is the *reciprocal* of the fractional part from the line before.
Check that this procedure results in the continued fraction

$$\frac{191}{23} = 8 + \frac{1}{3 + \frac{1}{3+\frac{1}{2}}}$$

Now check that, if we stop short of the next $\frac{1}{}$ at each level, we get a succession of ever better approximations

$$8, \quad \frac{25}{3}, \quad \frac{82}{10}, \quad \frac{191}{23}$$

And notice that each of these approximations was in the sequence in the Brocot Excursion but that the continued fraction gets there much faster.
b) The successive values of the general continued fraction at the start of this Excursion (which we can write $[a_0, a_1, a_2, a_3, \cdots]$) are

$$\frac{p_0}{q_0} = \frac{a_0}{1}, \quad \frac{p_1}{q_1} = \frac{a_1a_0+1}{a_1}, \quad \frac{p_2}{q_2} = \frac{a_2a_1a_0 + a_0 + a_2}{a_2a_1+1} = \frac{a_2p_1+p_0}{a_2q_1+q_0}$$

$$\frac{p_3}{q_3} = \frac{a_3a_2a_1a_0 + a_1a_0 + a_3a_0 + a_3a_2 + 1}{a_3a_2a_1 + a_a + a_3} = \frac{a_3p_2+p_1}{a_3q_2+q_1}, \quad \cdots$$

The pattern suggests we can calculate successive approximations, p_j/q_j, as we go along in the same table that gave us f, $\lfloor f \rfloor$, etc. This will help us when we don't want to recalculate the original fraction exactly but will be happy to stop with some suitable approximation.
c) A simple example of a continued fraction which goes on forever, on the other hand, is the "Golden ratio", ϕ, which we'll meet in Excursion *Golden ratio* of Week ii (based on "Fibonacci numbers" of Note 2 of that Week ii). All we need to know now is

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

This suggests we can replace the ϕ in the denominator by this same expression

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

And again

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

And again and again forever

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

We will find in Week ii that ϕ is there calculated as an infinite process of finding ratios—it is not a rational number because we never stop finding the ratios.
d) Let's try another number which cannot be expressed as a simple ratio: the square root of 2. Here's the table starting with $\sqrt{2} = 1.4142\cdots$.

f	$\lfloor f \rfloor$	fracpart(f)
$1.4142\cdots$	1	$0.4142\cdots$
$2.4142\cdots$	2	$0.4142\cdots$
$2.4142\cdots$	2	$0.4142\cdots$
:	:	

So the continued fraction appears to be

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \cdots}}}$$

How do we know $1/(\sqrt{2} - 1) = \sqrt{2} + 1$ (which you can see we seem to have needed to go from fracpart(f) in any line of the table to f in the next line)? Just multiply top and bottom of the fraction by the same thing, $\sqrt{2} + 1$:

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

48. **Making fractions clear.** One day, Mamma Bear baked a pie. It smelled so good when she took it out of the oven that she ate a piece without waiting for Papa Bear to come home with Baby Bear from the daycare. She was careful to eat only her share, 1/3 of the pie.
a) What fraction of the pie was left over?
b) What fraction of the left-over piece did Mamma Bear reasonably expect Papa Bear to have? What fraction of the whole pie was that?
c) When Papa Bear got home with Baby Bear he actually sat down and ate 1/2 of the original whole pie. What fraction of the whole pie did that leave for Baby Bear?
These questions illustrate three important things about fractions: complements, products and sums (or differences).
a) The *complement* of a fraction p/q is $(q - p)/q$. So the complement of 1/3 is 2/3. It is the "left-over" after eating 1/3 of the pie.
b) The *product* of two fractions p/q and r/s is $(pr)/(qs)$. So if Mamma Bear expected Papa Bear to share the 2/3 pie equally with Baby Bear, that would be 1/2 of 2/3: (1/2)*(2/3) = (1*2)/(2*3) = 2/6 = 1/3.
This last step illustrates a fourth important thing about fractions, *reduction to lowest terms.* To see this it is easiest to start *before* doing the multiplications top and bottom. In (1*2)/(2*3) we can "cancel" the two 2s, so (1*2)/(2*3) = 1/3. So if top and bottom have a common *divisor* (2 in this case) we can get rid of it from both top and bottom.
c) The *difference* of two fractions is a little more complicated. We must adjust each fraction so that both have the same denominator. Then we can subtract the two new numerators.
The adjustment is the opposite of reduction to lowest terms: we must multiply both top and bottom of each fraction in such a way that the two adjusted fractions both have the same denominator. The simplest way is just to use the denominator of the other fraction.
Here it is for greedy Papa Bear. Mamma Bear had left 2/3 of the pie and Papa Bear ate 1/2 of the pie. That leaves (2/3) − (1/2) of the pie for Baby Bear.

$$\frac{2}{3} - \frac{1}{2} = \frac{4}{6} - \frac{3}{6} = \frac{4 - 3}{6} = \frac{1}{6}$$

We had to give the same denominator to 2/3 and 1/2 which we did by multiplying the two denominators, 2*3 = 6. So 2/3 is 4/6 and 1/2 is 3/6, and then we can subtract.
To add fractions we do the same thing, only add the numerators at the end. In terms of letters, to give the general pattern,

$$\frac{p}{q} + \frac{r}{s} = \frac{ps}{qs} + \frac{rq}{sq} = \frac{ps + rq}{qs}$$

(The two denominators might share a common divisor, in which case we can multiply by smaller numbers. Try adding (1/2) + (1/4) = (2/4) + (1/4).)
d) Express the complement of p/q as the difference between two "fractions", $1 - (p/q)$.

49. **Coprimes and greatest common divisor.** When a fraction is reduced to lowest terms, its numerator and denominator are "coprime" (or "relatively prime"): their only common divisor is 1.
This is a relative condition, and looser than "prime" in which the only *divisor* is 1 (and the number itself). Why are two prime numbers coprime? Why is *any* number coprime with a prime number? Well, any positive number less than the prime.
So to reduce fractions it is important to be able to find their *greatest common divisor.* We then divide top and bottom by that.
What is the greatest common divisor of 2 and 3? 2 and 4? 12 and 15? 10 and 27? Which of these pairs of numbers are coprime?
How many numbers less than 15 are coprime with 15? with 13? with any prime p?

50. **Modular arithmetic and Euclid's algorithm.** If g is the greatest common divisor of two numbers p and q then it is also the greatest common divisor of the smaller of these numbers and the *remainder* when the larger one, say q, is divided by the other:

$$q = pm + r$$

where m is the *multiple* that q is of p and r is the remainder (0 when the division is exact). Certainly g divides r or else q/g would not be an integer but we said it is. Furthermore, if r and p have a larger common divisor than g then so must q but we said that g is the largest common divisor of p and q.
Euclid captured this by saying (we'll need to refine it slightly below in the Excursion *Euclid's algorithm*)

$$\gcd(p, q) = \gcd(q \bmod p, p)$$

where q mod p is the mathematician's way of writing the remainder when q is divided by p. So "remainder arithmetic", or *modular arithmetic*, may be important in reducing fractions, to find the GCD.
We can make addition, multiplication and exponentiation tables for modular arithmetic. Here are two examples, modulo 4 and modulo 5.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

ˆ	0	1	2	3	4	..
0	1	0	0	0	0	
1	1	1	1	1	1	
2	1	2	0	0	0	
3	1	3	1	3	1	

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

ˆ	0	1	2	3	4	5	..
0	1	0	0	0	0	0	
1	1	1	1	1	1	1	
2	1	2	4	3	1	2	
3	1	3	4	2	1	3	
4	1	4	1	4	1	4	

Work out the similar tables for modulo 6 and modulo 7. How would you use modular arithmetic to find out what day of the week Monday plus nine is?

Note that addition always has an inverse—there is a zero in every row and every column of the "+" tables—but that multiplication only always has an inverse modulo a prime number (such as 5, where there is a one in every row and every column of the "×" table).

This observation helps us answer the *al jabr* question: can you do anything to a modular-arithmetic equation as long as you do the same thing to both sides? For division, the answer is "no", in general. Here are some examples to start your exploration.

a	0	1	2	3	4	5	6	7
a mod 4	0	1	2	3	0	1	2	3
$2a$	0	2	4	6	8	10	12	14
$(2a)$mod 4	0	2	0	2	0	2	0	2
$2(a$ mod 4)mod 4	0	2	0	2	0	2	0	2

a	0	1	2	3	4	5	6	7
a mod 4	0	1	2	3	0	1	2	3
$a/2$	0		1		2		3	
$(a/2)$mod 4	0		1		2		3	
$(a$ mod 4)/2 mod 4	0 or 2		1 or 3		0 or 2		1 or 3	

We see that multiplication agrees but that division, even where $a/2$ gives an integer result, is ambiguous mod 4 because of those repeats in the 2 row of the times table.

However, the 1 row and the 3 row of the modulo-4 times table are spared this problem, and there is a *cancellation rule*: if k and m are coprime, (I'm using a new symbol for equality modulo m)

$$ak \overset{(m)}{=} bk \quad \text{implies} \quad a \overset{(m)}{=} b$$

How about the other arithmetic operations? When

$$a \overset{(m)}{=} b$$

do the following always hold for any nonnegative integers a, b and m?

$$a + x \overset{(m)}{=} b + x \qquad ax \overset{(m)}{=} bx \qquad a^x \overset{(m)}{=} b^x$$

51. **Euclid's algorithm.** In Excursion *Modular arithmetic and Euclid's algorithm* above we saw that

$$\gcd(p, q) = \gcd(q \bmod p, p)$$

for the greatest common divisor of two integers p and q.

Here we develop this equation into a computer program. The important observation is that, assuming $p < q$, the two numbers after the right-hand "gcd" are smaller than the corresponding numbers after the left-hand "gcd".

Another important observation is that if q mod $p = 0$ there is no remainder and q divides p exactly. In this case, $\gcd(p, q) = p$.

If we were to think of the above equation as a *recursive* definition of the computer function `gcd`, that function could be considered to execute along the lines of the following example. We'll use the labels `p` and `q` to represent the two numbers input into `gcd()` with a different line in the following table to represent the values each time we call `gcd()`. We start with `gcd(12,15)`.

	p	q	
gcd(	12	15	)
gcd(	3	12	)
gcd(	0	3	)

Line by line, what's happened is that we typed `gcd(12,15)` and the equation converted this to `gcd(15 mod 12,12)` = `gcd(3,12)`.

And it went around again, giving `gcd(12 mod 3,3)` = `gcd(0,3)`.

At this point we know that the GCD of 12 and 3 is 3. The computer can then work back up the invocations of `gcd()` to the very first one, simply reporting `3` each time, and that's the answer: gcd(12,15) = 3.

But we should have told the computer to stop when we get to the zero. That's easy: we'll put in a *conditional expression* which has the value given by the keyword `then` or the value given by `else` depending on what happens in the test condition. For example,

```
          y = if x>0 then 1 else −1
```

makes `y` equal 1 if `x` is positive, otherwise 0.

Here is Euclid's algorithm with the stopping condition.

```
          gcd(p,q) = if p=0 then q else gcd(q mod p,p)
```

What happens if $p > q$?. Let's start with `gcd(12,27)`.

	p	q	
gcd(	12	27	)
gcd(	15	12	)
gcd(	12	15	)
gcd(	0	3	)

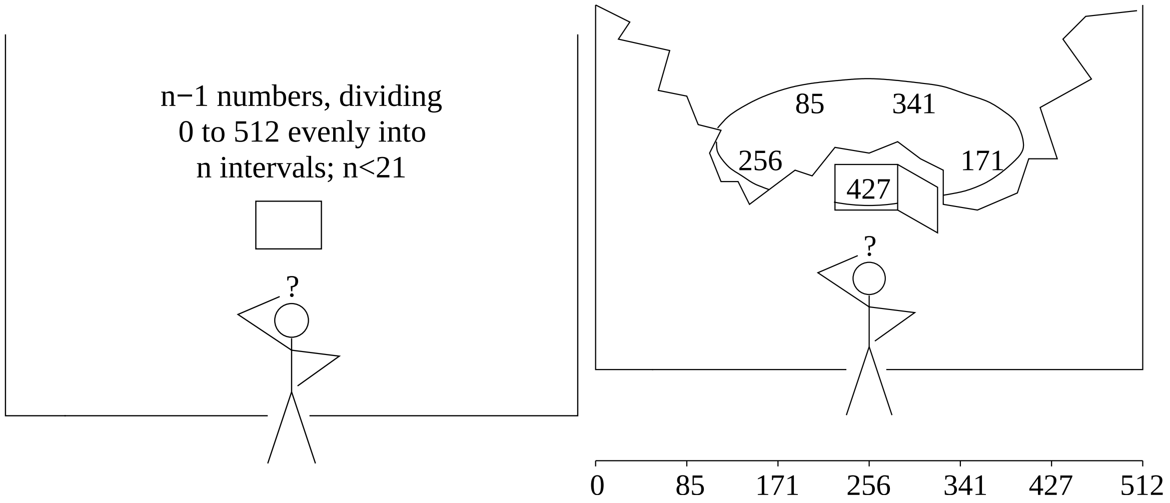
So it copes automatically.

Most modern programming languages can handle such recursion. It is not a circular definition of `gcd` the way it might seem. It is not an infinite regress because the numbers `p` and `q` get smaller and smaller and eventually `p` becomes 0 and the recursion stops.

It is also very easy to be sure that the program works the way we want. It depends only on the insight that p and q have the same GCD as q mod p and p, and on the fact that a zero remainder means the division is exact.

Write a MATLAB program for `gcd(p,q)`. Use `mod(q,p)` for q mod p. MATLAB supports recursion but has no conditional expression, so I often build `condif(cond,thn,els)` using `if-then-else` *statements*, just for elegance, but you can use conditional statements directly in `gcd()`.

52. **How many intervals?** a) How would you find out what n is if you were told that behind a window in a sealed cabinet there are $n-1$ numbers evenly dividing the range 0 to 512 into n intervals, and that n is not greater than 20? When the window is opened you can see only one of the numbers, which has been taken at random from the $n-1$.



The secret is the (almost) even spacing. The $n-1$ numbers will correspond to fractions of 512 whose denominators are n. So you should try to find the nearest fraction of 512 with denominator less than 21 that corresponds to the number shown. Excursion *continued fractions* should help. (Since we are looking for an approximation with $q < 21$ we include the successive numerators p and denominators q in the table: note that the rules given work only for $j > 1$ and consult Excursion *continued fractions* for the initial p_0, q_0, p_1 and q_1.)

f	$\lfloor f \rfloor$	fracpart(f)	$p_j = a_j p_{j-1} + p_{j-2}$	$p_j = a_j p_{j-1} + p_{j-2}$
$\frac{427}{512}$	0	$\frac{427}{512}$	0	1
$\frac{512}{427}$	1	$\frac{85}{427}$	1	1
$\frac{427}{85}$	5	$\frac{2}{85}$	5	6
$\frac{85}{2}$	42	—	211	253

You stop the process just before $q > 20$.
So the continued fraction approximating 427/512 to the largest denominator you are concerned about is

$$0 + \frac{1}{1 + \frac{1}{5}} = \frac{5}{6}$$

The denominator of this is 6. This suggests that there are $n = 6$ intervals (and so $n - 1 = 5$ numbers on the wheel inside the cabinet).
But you were lucky. Somebody else might have been shown 341, say.

f	$\lfloor f \rfloor$	fracpart(f)	$p_j = a_j p_{j-1} + p_{j-2}$	$p_j = a_j p_{j-1} + p_{j-2}$
$\frac{341}{512}$	0	$\frac{341}{512}$	0	1
$\frac{512}{341}$	1	$\frac{171}{341}$	1	1
$\frac{341}{171}$	1	$\frac{170}{171}$	1	2
$\frac{171}{170}$	1	$\frac{1}{170}$	2	3
$\frac{170}{1}$	170	—	341	512

This time the continued fraction is

$$0 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1}}} = \frac{2}{3}$$

And someone who saw 256 would arrive at the fraction 1/2.

So the best we can conclude is that n is some multiple of the denominator we get: in your case n could be 6 or 12 or 18, since any other multiple exceeds 20.

427 is not *exactly* 5/6 0f 512: how sensitive is this method to variations in the number shown? What if it had been 430 instead of 427? 420?

What is the *probability* the denominator we get *is* n? Well, when n was 6, all the possibilities are

fraction	$\frac{1}{6}$	$\frac{2}{6}$	$\frac{3}{6}$	$\frac{4}{6}$	$\frac{5}{6}$
denominator	6	3	2	3	6

once the fractions are reduced to lowest terms. So we get 6 correctly two out of five times or 40%: the probability is 0.4. But 6 has many divisors and few numerators that are coprime with 6 (see Excursion *Coprimes ..*).

Show that for a prime denominator, p, the probability of getting it right by this procedure is $(p-1)/(p-1) = 100\%$ Can you also show that if the denominator is the product of two primes, pq, then the probability is $(p-1)(q-1)/(pq-1)$? How does this check out with 6 above? How close does this get to 1 as p and q get big?

b) Clearly the number of coprimes of a number N, which are less than N, is important for this analysis. This function of N has a name, *Euler's totient function*, $\phi(N)$, and Leonhard Euler (pronounced "oiler": he's German) found a formula for it

$$\phi(N) = N \prod_{p|N} \left(1 - \frac{1}{p}\right)$$

which includes taking a product over all prime factors of N, i.e., primes p that divide N, $p \mid N$. For example

$$\phi(6) = 6\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 6\frac{1}{2}\frac{2}{3} = 2 \times 3 \times \frac{1}{2} \times \frac{2}{3} = 1 \times 2 = 2$$

Here we see the $p-1$ term we got for prime factor p above, in the component $p(1-1/p) = p(p-1)/p = p-1$.

The totient function has three properties which lead to this formula.

$$\begin{array}{rcll} \phi(p) & = & p-1 & p \text{ prime} \\ \phi(p^k) & = & p^{k-1}(p-1) & p \text{ prime} \\ \phi(mn) & = & \phi(m)\phi(n) & m, n \text{ coprime} \end{array}$$

To see the last we need the *Chinese remainder theorem* (Sun Tzu 3rd century AD) which says that, if m and n are coprime then all the numbers less than mn have a unique mapping to pairs taken from all the numbers less than m and all the numbers less than n. Here are illustrations for $6 = 3 \times 3$ and $12 = 3 \times 4$.

$a_1 \backslash a_2$	0	1	2
0	0	4	2
1	3	1	5

$a_1 \backslash a_2$	0	1	2	3
0	0	9	6	3
1	4	1	10	7
2	8	5	2	11

Here, a_1 ranges through all the numbers from 0 to $2-1$ ($3-1$ in the table on the right) and a_2 ranges through all the numbers from 0 to $3-1$ ($4-1$). In the body of each table you can find uniquely every number from 0 to $6-1$ ($12-1$) so that each of these numbers maps uniquely to a pair (a_1, a_2) and vice-versa.

Now if we look inside the table at numbers coprime to mn, which must clearly be coprime to both m and n, we can see that the count of these numbers is the product of the counts of a_1 which are coprime with m and the count of a_2 which are coprime with n.

$a_1 \backslash a_2$	0	1	2
0	0	4	2
1	3	1	5

$a_1 \backslash a_2$	0	1	2	3
0	0	9	6	3
1	4	1	10	7
2	8	5	2	11

The enlarged numbers are coprimes of m, n and mn appropriately. The shapes make the product rule evident. Can you go from here to a proof?
What is the 3D pattern of all the numbers less than N when N has *three* mutually coprime divisors?
Try some examples to convince yourself of the rule for p^k.
The prime-power rule and the product rule should now take you to Euler's formula, given that any number N can be factored into powers of primes, e.g., $12 = 2^2 \times 3^1$ so $\phi(12) = 2 \times (2-1) \times (3-1) = 4$.

53. **Fermat and Euler on modular powers.** From the multiplication table modulo 5 in Excursion *Modular arithmetic..* you can see that multiplying all numbers less than 5 by any given number just gives back the same set of numbers less than 5: each row of the × table is just a permutation of the numbers less than 5. It should be apparent that this must be the case for any prime p, not only 5. In particular, leaving the 0 out of that set,

$$a \times \{1, 2, \cdots, p-1\} \overset{(p)}{=} \{1, 2, \cdots, p-1\}$$

Multiplying them all together on each side

$$a^{p-1}(p-1)! \overset{(p)}{=} (p-1)!$$

Because p is prime we are allowed to cancel the $(p-1)!$ (see Excursion *Modular arithmetic..*) and we have "Fermat's little theorem"

$$a^{p-1} \overset{(p)}{=} 1$$

From the multiplication table modulo 4 in Excursion *Modular arithmetic..* you can see that multiplying all numbers less than 4 by any given number *which is coprime with 4*, i.e., 1 or 3, just gives back the same set of numbers less than 4: rows 1 and 3 of the × table are just permutations of the numbers less than 4. In general for modulus other than 4, if we select only columns which are also coprime with the modulus we can generalize Fermat's theorem, as Euler did.

$$a \times \{1, \cdots\} \overset{(m)}{=} \{1, \cdots\}$$

where a is coprime with m and the sets now contain only numbers coprime with m. Multiplying them all together on each side

$$a^{\phi(m)}\Pi \overset{(m)}{=} \Pi$$

where $\phi(m)$ is the *totient function* of m (see part (b) of Excursion *How many intervals?*) and Π is the product of all numbers smaller than and coprime to m.
Because Π is the product of coprimes, it is coprime itself and may be cancelled. So if a and m are coprime,

$$a^{\phi(m)} \overset{(m)}{=} 1$$

This *Euler-Fermat* theorem clearly incorporates Fermat's little theorem.

54. **Secret codes and encryption.** Most ciphers require modular arithmetic. Let's start with the Caesar cipher, which just shifts each letter in a message up by 3: a goes to d, b goes to e, etc., and, of course the end of the alphabet cycles back to the beginning. If we consider a minimal alphabet of 26 lower-case letters and one blank or space, an encryption might look like this.

w	e	l	c	o	m	e	⊔	t	a	x
23	5	12	3	15	13	5	0	20	1	24
26	8	15	6	18	16	8	3	23	4	0
z	h	o	f	r	p	h	c	w	d	⊔

I've used a convenient oxymoron as the message and represented blanks as ⊔. The encryption represents a-z as 1:26 and ⊔ as 0. It adds 3 modulo 27 to each of the numbers, then converts back again.

Note that the inverse, decryption, uses the same routine, but adding -3.

The Caesar cipher is easy to crack by *frequency analysis*. It is known that text in English typically contains more es than any other letter, followed by t then a and so on (etaonrish is what I remember and the frequencies diminish inversely proportional to the position of the letter in this sequence - "Zipf's law".)

So just looking at the cipher text we notice the only letter that occurs more than once is h. We try supposing that the cipher is a cyclic substitution cipher and that h stands for e, and we can decode it: z goes to w, h goes to e, and so on.

Of course, statistical methods require longer text and I did select this phrase from my favourites in a fortunate way. Here are some other short phrases you can explore.

```
  legal treason
  war on terror
 freakish beauty
 greedy altruism
 thermal refugee
absentee figurehead
peerless eyeglasses
```

Multiplying rather than adding might defeat the statistical methods, because different letters can map to the same letter.

welcome tax using ×3 instead of + 3 becomes ooiirlo fcr

(Note that the blank, ⊔, being represented as 0, remains blank.) Unfortunately, that property of ambiguous mapping means that modulo-multiplication cannot be inverted. We cannot *de*crypt.

How about exponentiation? The Euler-Fermat theorem (Excursion *Fermat and Euler on modular powers*) suggests we might be able to get an inverse. We need the totient function of our modulus, 27: $\phi(27) = \phi(3^3) = 3^2(3-1) = 18$. Euler-Fermat says that $a^{\phi(27)} \overset{(27)}{=} 1$ so $a^{k\phi(27)} = (a^{\phi(27)})^k \overset{(27)}{=} 1^k = 1$ for any positive integer k (*al jabr* rules for modular arithmetic—Excursion *Modular arithmetic ..*), and so, further, $a^{k\phi(27)+1} \overset{(27)}{=} a$. That is, it is possible to get a back again by raising it to a certain power modulo 27 (or any m). The power must be a multiple of $\phi(27) = 18$ plus 1, i.e., any number n such that $n \overset{(18)}{=} 1$. But we'd like this n to have divisors, so that we can use one divisor to encrypt and then the other divisor to decrypt—their product being n, the power that brings a back to itself again. So we try multiples of 18 plus 1: 19 no, 37 no, 55 = 5*11.

When we encrypt using ^5

welcome tax becomes `bt   pt na`

(there are two blanks before `pt`) and if we decrypt using ˆ11

`bt   pt na` becomes `we   me ta`

What happened? Look back at the numeric values for `welcome tax`: only `w`, `e`, `m`, `t` and `a` are coprime with 27. Everything else is a multiple of 3 and $27 = 3^3$.

We'll have to try another base, one which has a couple of primes but no prime powers beyond 1. Let's double the alphabet, leaving room for upper case letters, too, and a couple of punctuation marks, from 27 to $55 = 5{\times}11$. $\phi(55) = 4 \times 10 = 40$ and multiples of 40 plus 1 are 41, 81, 121, 161, $\cdots$. Two of these are squares and $161 = 7{\times}23$[1].

The squares are interesting: the encryption and decryption routines are identical. This is called *symetric* encryption.

`welcome tax` becomes, raised to 9 modulo 55, `wtlVyBt eaM`

`wtlVyBt eaM` becomes, raised to 9 modulo 55, `welcome tax`

Similarly, using 11 as exponent modulo 55, `welcome tax` converts back to `welcome tax` via `lewUobe tax`—not so well disguised.

However, it is even more interesting to have a decryption key *different* from the encryption key, because then the encryption key can be made *public*.

This solves the problem we've had all along but haven't mentioned yet, namely that the key must be *shared* between sender and recipient. How can this be done securely? But with a public key, as Diffie and Hellman first proposed, the recipient can broadcast that key to anyone, saying "use this to encrypt a message: I'll keep the private part of the key and only I can decrypt your message". *How* to do this was discovered by Rivest, Shamir and Adelman (RSA).

`welcome tax` becomes, raised to 7 modulo 55, `lywPegy oaC`

`lywPegy oaC` becomes, raised to 23 modulo 55, `welcome tax`

The *public key* will be the two numbers 55 and 7. The *private key* will be the two numbers 55 and 23. Both 7 and 23 are obtained from $55 = pq$ the product of two primes, via its totient function $(p-1)(q-1)$. If the 55 were a big enough number, an attacker cannot find p and q because integer factorization requires too much computational work. So hey cannot find $\phi(pq) = (p-1)(q-1)$ or take the steps we took to find 7 and 23.

The MATLAB program I've been using to do the above letter-by-letter calculations invokes the following routine.

```
% function out = lettermod55(letter,op,arg)            THM            180803
% treating ' a-z' as integers 0:26, 'A-Z' as 27:52, '.,' as 53,54
% use  op  to combine with  arg  then convert back to characters
% Used by phrasemod55(phrase,op,arg) to encrypt the  phrase
function out = lettermod55(letter,op,arg)
letternum = double(letter);
if 96<letternum & letternum<123, letternum = letternum-96;            % a-z
elseif 64<letternum & letternum<91, letternum = letternum-64+26;      % A-Z
elseif letternum==32,letternum = 0;                                   % blank
elseif letternum==44,letternum = 54;                                  % ,
elseif letternum==46,letternum = 53;                                  % .
else
 display(['letternum ' num2str(letternum) ' out of range 32,44,46,65:90,97:122'])
```

[1] Looking for factors of these numbers, the *congruence class* $\overline{1 \bmod 40} = \{\cdots,-119,-79,-39,1,41,81,121,161,..\}$, would be as hard as the original problem. Instead, we choose one of the factors first, say e with $\gcd(e,40) = 1$, so e is one of the 16 numbers coprime with 40, $e \in \{1,3,7,9,11,13,19,21,23,27,29,31,33,37,39\}$. Then we find its *modular inverse*, say d with $de \overset{(40)}{=} 1$ and d is also coprime with 40. So if $e = 3$ then $d = 27$; if $e = 7$ then $d = 23$; if $e = 9$ then $d = 9$; if $e = 11$ then $d = 11$. Directly, given e, Euler-Fermat says $ed \overset{(40)}{=} 1$ so $ed = 1 + k\phi(55)$ for some integer k and we must only try different k until $d = (1 + k\phi(55))/e$. So for $e = 7$ we try 1,41,81,121,161,.. and the first to be divisible by 7 is $161 = 7 \times 23$.

```
end % if
switch op
case '+'
 letnumout = mod(letternum+arg,55);
case '*'
 letnumout = mod(letternum*arg,55);
case '^'
 letnumout = letternum;
 for j = 2:arg
  letnumout = mod(letternum*letnumout,55);
 end % for j
otherwise
 display(['op ''' op ''' not +, * or ^'])
end % switch
if 0<letnumout & letnumout<27, out = char(letnumout+96);                % a-z
elseif 26<letnumout & letnumout<53, out = char(letnumout+64-26);        % A-Z
elseif letnumout==0, out = ' ';                                         % blank
elseif letnumout==54, out = ',';                                        % ,
elseif letnumout==53, out = '.';                                        % .
end % if

% 180802
% lettermod55('a','+',1)        ans = b
% lettermod55('A','+',2)        ans = C
```

You can write the corresponding `lettermod27.m` as well as the invoking routines `phrasemod55.m` and `phrasemod27.m` respectively.
Of course, keys need not be applied to one letter at a time. Here is an example of applying a *keypad* using addition modulo the base (27 or 55).
`phrasekeypad('welcome tax',[1,2,3]) ans = xgodqpfbxbz`
and its inverse `phrasekeypad('xgodqpfbwbz',-[1,2,3]) ans = welcome tax`
We see that the repeated letters, `b`, in the ciphertext are spurious and will not help statistical analysis. If the keypad were the length of the entire message, and random, and used *for the one message only*—a *one-time* keypad—the message would be uncrackable, as Shannon showed.
But the key must still be shared.
So how about using RSA to *distribute a one-time keypad* which is then used for the single message?

55. **Cracking RSA.** The Rivest-Shamir-Adelman public-key encryption technique introduced in Excursion *Secret codes and encryption* relies for its security on the difficulty of factoring large integers. Basically one must try all the prime numbers up to the square root of the number to be factored, just as in checking for primacy. Well, there is another way, but, short of quantum computing, it is also very expensive. It involves the Fourier transform, which we meet in Week 9, so the present Excursion is incomplete until we get to Week 9 and Book 11d. In Excursion *Modular arithmetic ..* we calculated tables of exponentials modulo various bases. Look back and note that, if the base is prime, in those tables the rows a^b for $b = 0, 1, 2, \cdots$ are *periodic.* And if the base is not prime, rows associated with values of a coprime with the base are also periodic. The periods vary and I presume there is no rule for finding them other than calculating. (To calculate these exponentials, don't try `mod(a^b, base)` but take advantage of *al jabr* and write a loop `x = a; for j=2:b, x = mod(x*a,base); end`. Why? Could it be done better?)

Now if for a coprime with the base the period is q, that means that $a^q \overset{\text{(base)}}{=} 1$ or $a^q - 1 \overset{\text{(base)}}{=} 0$. That is, $a^q - 1$ is a multiple of `base`, containing both its factors. If q is even, $(a^{q/2}+1)(a^{q/2}-1) \overset{\text{(base)}}{=} 0$. If $a^{q/2}-1 \overset{\text{(base)}}{=} 0$ then $a^{q/2}-1$ is a multiple of `base`—and $(a^{q/2}+1)$ is coprime to `base` and so contains neither factor. Otherwise, the two factors of `base` may separate, with one in $(a^{q/2}+1)$ and the other in $a^{q/2}-1$, and can be discovered by taking the gcd with `base`.
Let's try this with base 21 (a little more tractable than base 55 in Excursion *Secret codes and encryption*, but you can try that base yourself next). Here are all the $\phi(21) = 12$ coprimes smaller than 21, their periods and the sequences within those periods.

a	period q	sequence
1	1	1,1$\cdots$
2	6	1,2,4,8,16,11,1$\cdots$
4	3	1,4,16,1$\cdots$
5	6	1,5,4,20,16,17,1$\cdots$
8	2	1,8,1$\cdots$
10	6	1,10,16,13,4,19,1$\cdots$
11	6	1,11,16,8,4,2,1$\cdots$
13	2	1,13,1$\cdots$
16	3	1,16,4,1$\cdots$
17	6	1,17,16,20,4,5,1$\cdots$
19	6	1,19,4,13,16,19,1$\cdots$
20	2	1,20,1$\cdots$

Nine of these 12 coprimes have even periods. Those with period 6 (a = 2, 5, 10, 11, 17, 19) invite us to check $a^3 \pm 1 = 8 \pm 1$ (a = 2, 11), $a^3 \pm 1 = 13 \pm 1$ (a = 10, 19) or $a^3 \pm 1 = 20 \pm 1$ (a = 5, 17). From these we get 7, 14 and 21 respectively, and the GCD of the first two with 21 give us the factor 7. For example, 8 − 1 = 7, or 13 + 1 = 14 and GCD(14,21) = 7.
Those with period 2 (a = 8, 13, 20) lead to $a^1 \pm 1 = 8 \pm 1$(a= 8), to $a^1 \pm 1 = 13 \pm 1$(a= 13) and to $a^1 \pm 1 = 20 \pm 1$(a= 20), giving factor 7 in the same ways as before.
And the eight that are not coprime with 21 (a = 3, 6, 7, 9, 12, 14, 15, 18) give, from GCD(a,21), the factor 3 or the factor 7.
What we do, then, is to select a number less than 21 at random and take its GCD with 21. Either the number is a factor or the GCD is 1. In the first case, we're done. In the second case we must find the period q such that $a^q \overset{(21)}{=} 1$ and then check $a^{q/2} \pm 1$. Except where the half-period gives 21 as a "factor" (three lines out of 20 numbers in all), or the period is not even (another three), this process will give a result. When it fails, we just take another number at random and try again. In this example, there is a 70% chance of success with one try; two tries reduce the chance of failure to 9% and three tries to 3%.
The expensive part of this process is finding the period. The Fourier transform (Week 9) converts a function with period q to another function essentially zero except at the ends of q regularly-spaced intervals. We can use the continued-fraction techniques of Excursion *How many intervals?* to guess the period, then try it out using the $a^{q/2} \pm 1$ tricks above.
Try this, supposing various results from the random selection: 18, 4, 20, 10.
A *quantum Fourier transform* (Book 11d) speeds up this part of the process enough to make the whole thing feasible. So a quantum computer will be able to crack RSA.

56. **Fermat's little theorem again.** An important interpretation of the exponential a^m is that this is the number of patterns of length m we can get out of an alphabet of a characters. Suppose $a = 2$ and the two characters are `A` and `B`. Then all the patterns of length $m = 3$ are

```
AAA
AAB
```

```
ABA
BAA
ABB
BAB
BBA
BBB
```

There are $a^m = 2^3 = 8$ of them.
Notice that there are four groups: `AAA` and `BBB` with all letters the same, the group of three with two `A` and one `B`, and the group of three with one `A` and two `B`. So

$$2^8 \bmod 3 = (1 + 3 + 3 + 1) \bmod 3 = 1 + 0 + 0 + 1 = 2$$

Convince yourself that such an argument holds for any prime m and you have another proof of Fermat's little theorem (Excursion *Fermat and Euler on modular powers*)—although a proof which does not extend to the Euler-Fermat theorem.

57. (Eugene Lehman) How many times and exactly when do the hour and minute hands coincide on an analog clock, starting at one second after midnight and ending the following noon?
a) Try an approximate solution to start with, by saying to the nearest minute what time the first coincidence will occur. (Not at midnight, since we are starting just after the midnight coincidence.) Then step this forward, stopping before you go past noon.
b) By how much does this approximation get wrong the last coincidence before noon? What corrections to all the other coincidence timings will fix this error? Confirm that the final coincidence is exactly at noon. Work with fractions for this part.
c) Repeat (b) but this time work with decimals. You will need a way of writing infinitely repeating decimals. A convention is the bar: $0.232323.. = 0.\overline{23}$. Be careful when adding two infinitely repeating decimals written this way.
d) Check your work in (c) by calculator, which should show enough decimal places to give the right idea.

58. a) Invent and work through a number of examples of temperature drops and rises, across 0°C, above 0°C and below 0°C, until you are comfortable with working with negative arithmetic. How would you interpret and calculate a drop of -8C°? a rise of -8C°?
b) Martin Gardner imagined a room full of good and bad people. He supposed that adding is sending people into the room and subtracting is calling people out of the room. He supposed that good people are positive and bad people are negative. Thus adding $+5$ to the room sends in 5 good people, while adding -5 sends in 5 bad people. Subtracting $+5$ calls out 5 good people and subtracting -5 calls out 5 bad people.
Multiplying by $+3$ is adding 3 times. Multiplying by -3 is subtracting 3 times. So $(-3)\times(-5)$ successively subtracts -5 3 times, thereby *in*creasing the goodness of the room by 15 people. Work through several examples of this "model" of arithmetic.
c) Find and practice with some other "model"s of negative arithmetic—ones, for instance, which might be suitable for people who do not live in climates where the temperature can drop below freezing. Can you find any persuasive ones which involve placing the numbers along a straight line and reversing direction for multiplication by -1? (Hint. Look up Margaret Atwood's CBC Massey Lectures, 2008, Toronto, House of Anansi Press.)
d) What is $2 \times -4 \times 3 \times -6 \times -7$? Why does an odd number of negative values in a product give a negative result? Why does an even number of negative values in a product give a positive result?

59. a) Modify the `railwayTracks` program, or the corresponding plot on your calculator, to explore a variety of slopes and separations of straight-line ("linear") equations. Can you work out a rule for the value of `X` that makes `Y = 0`? (If you use the `TRACE` button and the

arrow keys on your calculator, you can display values of `X` and `Y` to test your rule.)
b) What constant must be added to a line of slope s to give a second line, also of slope s but a distance a apart from it, measuring the distance perpendicular to the two lines, as in Note 11?

60. a) Write and run a calculator program to plot the nonlinear expressions of Note 12.
b) What are the rules for finding the values of `X` that make `Y = 0` in the nonlinear plots of Note 12?
c) The general form of a "quadratic" expression is aX^2+bX+c, and of a "cubic" expression is AX^3+BX^2+CX+D. Work out the values of a, b and c for the triangular and square number expressions. Work out the values of A, B, C and D for the tetrahedral number expression.
d) Using the expression `2X + c` in a plotting program, find c by trial and error so that this straight line just touches the $\texttt{X}^2$ curve at `X = 1`. (The straight line is then said to be "tangent" to the curve, and its slope, 2, is the slope of the curve at the point of tangency.

61. At most and at least how many times do linear, quadratic and cubic expressions cross the horizontal $y = 0$ line? *Any* horizontal line?

62. Ramanujan called the integers his friends. Now we know enough about the integers to begin to give each one a "personality". We can do this by noting whether or not the integer is prime, is a triangular number, is square, is a sum of squares, and so on.
Make a table such as the following, with all the possible properties of integers discussed in these Notes, and fill it out for as many integers as you like. Can you find two integers with identical "personalities", i.e., the same columns have $\surd$s in them?

	...	odd	prime	$\triangle$	$\square$	cube	$\sqrt[2]{}$	$\sqrt[3]{}$	$\square + \square$	hexag	tetrahed	..
1		$\surd$		$\surd$	$\surd$	$\surd$	$\surd$	$\surd$		$\surd$	$\surd$	..
:		:	:	:	;	:	:	:	:	:	:	

63. Any part of the Preliminary Notes that needs working through.

References

[Cox63] H. S. M. Coxeter. *Regular Polytopes.* The MacMillan Company, Collier-MacMillan Ltd, New York, London, 1963. 2nd ed.

[Der03] John Derbyshire. *Prime Obsession: Bernhard Riemann and the Greatest Unsolved Problem in Mathematics.* Penguin Group (USA) Inc, New York, 2003.

[Hay08] Brian Hayes. *Group Theory in the Bedroom, and Other Mathematical Diversions.* Hill and Wang (Farrar, Straus and Giroux), New York, 2008.