CHAPTER 8
Greatest Common Divisor

If A and B are integers (whole numbers) then a *common divisor* (or *common factor*) of A and B is an integer which divides both numbers. And, the greatest common divisor (or highest common factor) of A and B is the largest such integer.

For instance, 3 is a common divisor of 12 and 18. But 6 is the greatest common divisor of 12 and 18.

Calculating the greatest common divisor of two numbers is not particularly complicated. Especially for a computer. The method employed serves as a good illustration of a computational algorithm.

The Euclidean algorithm is the most well-known and oldest (third century B.C.) method of computing the greatest common divisor. If you want to find the greatest common divisor of A and B then the procedure is as follows.

1. Rename A and B (if necessary) so that A is greater than B.
2. Divide A by B and find the remainder R1.
   R_1 = A MOD B

Notice that every number that divides A and B also divides R_1. And, conversely, every common divisor of B and R_1 is also a divisor of A. It follows that the common divisors of A and B are the same as those of B and R_1. Thus the greatest common divisor of A and B equals the greatest common divisor of B and R_1.

3. Now divide B by R_1 and find the remainder R_2.
   R_2 = B MOD R_1

The remarks made above between the numbers B, R_1 also apply to R_1, R_2. Thus the greatest common divisor of A and B equals the greatest common divisor of R_1 and R_2.

4. Next, divide R_2 by R_1 to get a remainder R_3.
   R_3 - R_1 MOD R_2

The process is continued in this manner until the remainder is zero. Notice that the remainders are decreasing on each occasion and so reach zero after a certain number of steps.

$R_1 = A \text{ MOD } B \qquad (0 <= R_1 < B)$
$R_2 = B \text{ MOD } R_1 \qquad (0 <= R_2 < R_1)$
$R_3 = R_1 \text{ MOD } R_2 \qquad (0 <= R_3 < R_2)$
• •
• •
• •
$R_{N-1} = R_{N-3} \text{ MOD } R_{N-2} \qquad (0 <= R_{N-1} < R_{N-2})$
$R_N = R_{N-2} \text{ MOD } R_{N-1} \qquad (R_N = 0)$

When the remainder reaches 0 we see that the previous remainder R_{N-1} is the greatest common divisor of R_{N-1} and R_{N-2}. Arguing in this way we see that R_{N-1} is the greatest common divisor of A and B.

The process outlined above is easily computerised. A program doing this is given below.

Listing 3.1

```
LIST
   10 REM Greatest common divisor
   20 MODE 1:COLOUR 3:PRINT ' TAB(3);"Gr
eatest common divisor"':@%=10
   30 PRINT "This program calculates the
 greatest    common divisor of two integ
ers using theEuclidean algorithm."'
   40 COLOUR 1:PRINT '"Enter the two int
egers:"
   50 REPEAT
   60  INPUT '" First integer: ";A%
   70  PRINT " First integer is ";A%
   80  IF A%<1 THEN COLOUR 3:PRINT '"A p
ositive integer please.":COLOUR 1
   90 UNTIL A%>0
  100 REPEAT
  110  INPUT '"Second integer: ";B%
  120  PRINT "Second integer is ";B%
  130  IF B%<1 THEN COLOUR 3:PRINT '"A p
ositive integer please.":COLOUR 1
  140 UNTIL B%>0
  150 IF A%<B% THEN C%=A%:A%=B%:B%=C%
  160 REM The Euclidean algorithm
```

```
  170 R%=A%:S%=B%
  180 REPEAT
  190  TEST=-1
  200  T%=R% MOD S%
  210  IF T%<>0 THEN R%=S%:S%=T%:TEST=0
  220 UNTIL TEST
  230 COLOUR 2:PRINT '"The greatest comm
on divisor is: ";
  240 IF LEN(STR$(S%))>8 THEN PRINT
  250 PRINT ;S%
  260 PRINT '"The least common multiple
is: ";
  270 T=A%*B%/S% : REM Used in case of l
arge numbers
  280 IF T>&7FFFFFFF AND LEN(STR$(T))>10
 THEN PRINT
  290 IF T<=&7FFFFFF THEN T%=A%*B%/S% EL
SE T%=1
  300 IF LEN(STR$(T%))>10 THEN PRINT
  310 IF T>&7FFFFFF THEN PRINT ;T ELSE P
RINT ;T%
  320 COLOUR 3:PRINT CHR$(7) '' TAB(10);
"Another go? Y or N ";
  330 REPEAT:G$=GET$:UNTIL G$="Y" OR G$=
"N"
  340 IF G$="Y" THEN RUN
  350 CLS:PRINT '"Bye for now.":END
```

RUN

```
   Greatest common divisor

This program calculates the greatest
common divisor of two integers using the
Euclidean algorithm.


Enter the two integers:
```

```
 First integer: ?148
 First integer is 148

Second integer: ?259
Second integer is 259

The greatest common divisor is: 37

The least common multiple is: 1036


          Another go? Y or N
```

The program also calculates the least common multiple of A and B. The least common multiple of two numbers A and B is the smallest number which is divisible by both A and B. The value of the least common multiple of A and B is given by

A*B/(greatest common divisor)

If the greatest common divisor of A and B is D then it is possible to write D as a combination of A and B:

D = S*A + T*B

where S and T are integers. The values of S and T can be found by working backwards with the Euclidean algorithm. Modify the greatest common divisor program so that it also computes S and T.