

## Euclid's Algorithm

### Background

#### The Distributive Property:

The distributive property is key to why Euclid's Algorithm works. Below it is illustrated with a specific example. Think about *how* to generalize this example.

3 is a *factor* (or *divisor*) of 18 (or we say 3 *divides* 18) because  $18 \div 3$  has no remainder.

Visually, we can represent 18 as groups of 3:



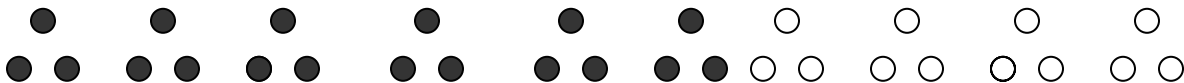
As an equation, we have  $18 = 6 \cdot 3$ .

Now, 3 is also a factor of 12, because  $12 \div 3$  has no remainder. Visually we have,



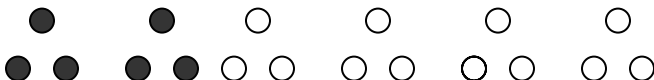
and as an equation we have,  $12 = 4 \cdot 3$ .

Now, the distributive property tells us that 3 is a factor of both  $18+12$  and of  $18-12$ . Visually, we see that  $18+12$  can be written as  $6+4=10$  groups of 3:



As an equation, we have  $18+12 = 6 \cdot 3 + 4 \cdot 3 = (6+4) \cdot 3 = 10 \cdot 3$ .

Similarly,  $18-12$  can be written as  $6-4=2$  groups of 3:



As an equation, we have  $18-12 = 6 \cdot 3 - 4 \cdot 3 = (6-4) \cdot 3 = 2 \cdot 3$ .

For understanding Euclid's Algorithm, the important consequence of the distributive property is that if  $f$  is a factor of both  $a$  and  $b$ , then  $f$  is a factor of both  $a + b$  and of  $a - b$ .

### **An Illustration of Euclid's Algorithm (first version):**

We will find the greatest common factor of 72 and 30. The *greatest common factor* is exactly what it sounds like: it is the largest natural number that is a factor of both 30 and 72.

By the distributive property, we know that any factor of both 72 and 30 is also a factor of  $72 - 30 = 42$ .

Similarly, any factor of both 30 and 42 is also a factor of  $42 - 30 = 12$  (and thus, any factor of both 72 and 30 is also a factor of 12).

Continuing in this manner, any factor of both 30 and 12 is also a factor of  $30 - 12 = 18$ .

Any factor of both 18 and 12 is also a factor of  $18 - 12 = 6$ .

Any factor of both 12 and 6 is also a factor of  $12 - 6 = 6$ .

Now we are left with 6 and 6. Following the entire chain of reasoning above, any factor of both 72 and 30 must also be a factor of 6.

Now, the greatest factor of 6 is 6 itself. So, if we can show that 6 must be a factor of 30 and 72, then 6 must be the greatest common factor of 30 and 72. Of course, 6 is a factor of both 30 and 72, but to use this example to illustrate how to prove that Euclid's Algorithm works in general, we note that we can use the distributive property looking at the algorithm *backwards*. Since 6 is a factor of both 6 and 6, it is a factor of  $6 + 6 = 12$ . Since 6 is a factor of 6 and of 12, it is a factor of  $6 + 12 = 18$ , etc. Continuing this way, we see that 6 is a factor of both 30 and 72, hence it is the greatest common factor.

**Notation:** We write  $\text{GCF}(30,72)=6$  or  $\text{GCD}(30,72)=6$  or just  $(30,72)=6$  (The Stein book uses this latter notation).

### **Second Version:**

This version of Euclid's Algorithm is more compact, but a bit trickier. It depends on the division algorithm, that is, for any natural numbers,  $a$  and  $b$ , with  $a \geq b$ , we can write  $a = b \cdot q + r$ , where  $q$  is the *quotient* and  $r$  is the *remainder*. For example,  $72 = 30 \cdot 2 + 12$ , when we divide 72 by 30, we have a quotient of 2 and a remainder of 12. Note that the first two steps in our previous example involved subtracting 30, until we had a remainder of 12; we can use the division algorithm to combine steps as follows:

$$\begin{aligned}72 &= 30 \cdot 2 + 12 \\30 &= 12 \cdot 2 + 6 \\12 &= 6 \cdot 2\end{aligned}$$

In each step we use the previous dividend (e.g. 30, then 12) and the previous remainder (e.g. 12, and then 6) for the next equation, we then find a new quotient and remainder.

Here is another example: Find the greatest common factor of 9768 and 4235:

$$9768 = 4235 \cdot 2 + 1298$$

$$4235 = 1298 \cdot 3 + 341$$

$$1298 = 341 \cdot 3 + 275$$

$$341 = 275 \cdot 1 + 66$$

$$275 = 66 \cdot 4 + 11$$

$$66 = 11 \cdot 6$$

Thus,  $(9768, 4235) = 11$ .

### **Explorations:**

1. Try both versions of Euclid's Algorithm, by hand, to find the greatest common factor of 219 and 123.
2. If you are new to Excel, or rusty, take a few minutes to go over the "Introduction to Spreadsheets" handout. The main things you need to know to set up Euclid's algorithm on a spreadsheet are how to use formulas and relative references.
3. Set up one of the versions of Euclid's algorithm on Excel. Then try to set up the other version. Helpful commands are MAX, MIN, and INT (for example, =MAX(A1,B1) gives the maximum of the values in cells A1 and B1, and =INT (A1/B1) gives the quotient of A1 divided by B1: INT (17/3)=5).
4. Read pages 44-46 of Stein, which describes how to solve many of the potato weighing problems using Euclid's algorithm. Use this method, and the first example above, to find integers M and N so that  $6 = 30M + 72N$ .
5. Challenge: Set up a spreadsheet on Excel to do Euclid's algorithm "backwards" to write the greatest common divisor of two natural numbers as a linear combination of those two numbers (i.e. to solve the potato problem, to do what you did in problem 4). To do this, study carefully how you get from one step to another in the examples in Stein or others you do by hand, and then see if you can change them into a recursive process. Use your spreadsheet to find M and N so that  $11 = 9768M + 4235N$ .
5. Go through the "Second Version" example carefully, explaining step by step, first why 11 must be a factor of both 9768 and 4235, and second why it must be the greatest common factor.

*Copyright 2005, Debra K. Borkovitz. You may copy or edit this material for non-profit, educational use only.*