Euclidean Algorithm

Kevin Li

January 2022

1 Divisibility

To start off the new quarter smoothly, let's jump into some concepts many of us should already be familiar with.

Definition 1. For integers a, b, we say a divides b if there exists x such that $b = xa$. We write $a|b$ to mean "a divides b".

Definition 2. The **Least Common Multiple** of two integers (usually nonnegative) a, b is the smallest number c such that $a|c$ and $b|c$. We will denote this by $c = lcm(a, b)$. The **Greatest Common Divisor** of a and b is largest number d such that $d|a$ and $d|b$. We will denote this as $gcd(a, b)$ or simply (a, b).

Problem 1. Compute the following:

$lcm(24, 32)$

$lcm(64, 27)$

$gcd(144, 312)$

$gcd(1071, 462)$

As the numbers get slightly larger, the time it states to compute LCM and GCD get significantly longer. For small numbers such as those in the above problem, there are many division tricks you can use to simplify calculations. However, with large numbers it is harder. Let's explore some ideas in number theory which will allow us to reduce computation time.

Definition 3. We say two integers a, b are **Relatively Prime** if $gcd(a, b) = 1$.

Problem 2. If a, b are natural numbers with $a|b$ and $b|a$ then what can we say about the relative size of a and b? Try to show it mathematically.

Problem 3. Let a, b, c be integers with $a|b$ and $b|c$. Show that $a|c$.

Problem 4. Let a, b, x, y be integers such that $a|b$ and $a|c$. Show that $a|xb + yc$.

If we recall the steps that we take to compute problems with LCM, GCD, and Relatively Prime, all of these require knowledge of **Prime Numbers**.

Definition 4. Let a be a natural number. The **Prime Factor Decomposition** of a is a product in the form $a = p_1^{e_1} p_2^{e_2} ... p_n^{e_n}$ where all $p_1, ..., p_n$ are distinct prime numbers.

Problem 5. Let a, b be natural numbers. Using Prime Factor Decomposition, find an explicit formula for $lcm(a, b)$ and $gcd(a, b)$.
HINT: Write out a general Prime Factor Decomposition for a,b. The following functions may be helpful:
$min(x, y) = \begin{cases} x & x \leq y \\ y & y \leq x \end{cases}$, $max(x, y) = \begin{cases} y & x \leq y \\ x & y \leq x \end{cases}$

2 Division Algorithm

Let's explore something that all of us have done in arithmetic probably without thinking about it very much. The division algorithm is a very simple and prevalent as the basis of many divisibility arguments.

Example 5. To illustrate this, lets take the numbers 7 and 61. To divide 61 by 7 while keeping the remainder, we simply calculate the largest multiple of 7 that is smaller than 61 and add on the remainder:

$$61 = 8 * 7 + 5$$

Though extremely simple, this is an extremely useful tool in reducing certain computations which we will see later in this worksheet.

Problem 6. CHALLENGE: Let a, b be natural numbers such that $a > b$. Show that there exists unique natural numbers q, r such that $0 \leq r < b$ and $a = qb + r$. (Note this is an exercise in proof writing called existence and uniqueness. If the existence part is too hard, skip it and try the uniqueness part. Have your instructor explain what this means.)

Definition 6. Let a, b be integers. A **Linear Combination** of a, b over the integers is a number in the form $xa + yb$ where x, y are integers.

Example 7. We can write 1 as a linear combination of 17 and 13, namely

$$1 = 4 * 13 - 3 * 17$$

Similarly, for general integers x, y clearly $-3x + 7y$ is a linear combination of x, y over the integers.

Problem 7. Let a, b be natural numbers. Suppose the smallest positive linear combination of a, b over the integers is d (i.e. $d = xa + yb$ for some integers x, y). Then show that $d = gcd(a, b)$. (**HINT:** Use the division algorithm to write $a = qd + r$ and remember the restriction r satisfies. Can you find a way to write r as a linear combination of a, b. You can do a similar process for b. Then to show d is the GREATEST common divisor, suppose there is another divisor c of both a, b. How can you show $c \leq d$?)

3 Euclidean Algorithm

Now that we have some practice with the division algorithm, we can introduce the **Euclidean Algorithm**. Before explaining it generally, let's see an example.

Example 8. Returning to problem 1, lets try to find $gcd(1071, 462)$ without relying on prime decomposition. We want to use the division algorithm to find q, r where $1071 = 462q + r$ where $0 \leq r < q$.

$$1071 = 2 * 462 + 147$$

Now, lets take the remainder 147 and use the division algorithm on 462, the smaller number we started with, and 147.

$$462 = 3 * 147 + 21$$

If we do this again, we find that

$$147 = 7 * 21 + 0$$

Therefore, this algorithm tells us that $gcd(1071, 462) = 21$ (check your answer!) More generally, let a, b be natural numbers with $a > b$. Using the division algorithm and the process described above, we have the following steps:

$$a = q_0 b + r_0$$

$$b = q_1 r_0 + r_1$$

$$r_0 = q_2 r_1 + r_2$$

$$r_1 = q_3 r_2 + r_3$$

$$\vdots$$

$$r_{n-2} = q_n r_{n-1} + r_n$$

This process continues until $r_n = 0$ in which case r_{n-1} is $gcd(a, b)$. (Remember, at each step $0 \leq r_{i+1} < r_i$)

Problem 8. Why is this algorithm guaranteed to stop?

Problem 9. Use the Euclidean Algorithm to find the following:

$gcd(93, 42)$

$gcd(537, 148)$

$gcd(2424, 144)$

Problem 10. Let a, b be natural numbers with $a > b$ and $a = qb + r$ where $0 \leq r < b$. Using problem 4, show that $gcd(a, b) = gcd(b, r)$. Does this explain why the Euclidean Algorithm works?

Problem 11. Explain why the Euclidean algorithm gives us a linear combination of the given numbers a, b (Refer to Example 8)