# Euclidean Algorithm

Kevin Li

January 2022

## 1 Extended Euclidean Algorithm

Recall from last week the Euclidean Algorithm:
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 $0 \leq r_{i+1} < r_i$).

**Theorem 1.** *Let $a, b$ be integers, and suppose $d = gcd(a, b)$. Then there exists $x, y$ integers such that $ax + by = d$. Such linear combination is minimal over the natural numbers.*

**Problem 1.** Suppose $a, b$ are natural numbers such that $gcd(a, b) = 1$ i.e. $a, b$ are relatively prime. How can we modify the above theorem for this specific case? In other words, using Theorem 1 on relatively prime numbers, what is the smallest positive linear combination $ax + by$?

**Problem 2.** As a bit of a reminder, compute the following using the Euclidean Algorithm:

1. $gcd(254, 32)$

2. $gcd(687, 24)$

3. $gcd(7544, 115)$

**Problem 3.** Try to find integers $x, y$ such that for given $a, b$, $ax + by = gcd(a, b)$

1. $a = 15$, $b = 23$

2. $a = 36$, $b = 21$

3. $a = 7544$, $b = 115$

**Example 2.** Now, since we are more familiar with the Euclidean Algorithm, we can introduce the Extended Euclidean Algorithm. It is an extension of the original algorithm, however it works backwards. Lets take a look at a numerical example:
Using Problem 2.2, we have the following steps in the usual Euclidean Algorithm to find $gcd(687, 24)$:

1. $687 = 28 * 24 + 15$
2. $24 = 1 * 15 + 9$
3. $15 = 1 * 9 + 6$
4. $9 = 1 * 6 + 3$
5. $6 = 2 * 3 + 0$

so we have that $gcd(687, 24) = 3$. The goal of the Extended Euclidean Algorithm is to use the steps of the Euclidean Algorithm **backwards** to find integers $x, y$ such that $687x + 24y = 3$.

1. $6 = 2 * 3 + 0 \rightarrow$ (Don't perform any operation here)

2. $9 = 1 * 6 + 3 \rightarrow 3 = 9 - 1 * 6$ (Write 3 in terms of the previous $a = 9, b = 6$)

3. $15 = 1 * 9 + 6 \rightarrow 6 = 15 - 1 * 9$
   $\rightarrow 3 = 9 - 1 * (15 - 1 * 9) = 2 * 9 - 1 * 15$
   (Do the same for the remainder of each line, substitute back to the previous step)

4. $24 = 1 * 15 + 9 \rightarrow 9 = 24 - 1 * 15$
   $\rightarrow 3 = 2 * (24 - 1 * 15) - 1 * 15 = 2 * 24 - 3 * 15$

5. $687 = 28 * 24 + 15 \rightarrow 15 = 687 - 28 * 24$
   $\rightarrow 3 = 2 * 24 - 3 * (687 - 28 * 24) = -3 * 687 + 86 * 24$

So we have found that $3 = -3 * 687 + 86 * 24$ where $x = -3, y = 86$.

**Problem 4.** Use the Extended Euclidean Algorithm to verify your solutions to Problem 3

1. $a = 15$, $b = 23$

2. $a = 36$, $b = 21$

3. $a = 7544$, $b = 115$

## 2 Number Theory

There are many different ways to apply the Theorems and Examples given on this worksheet alone. Let's apply these concepts to some ideas in number theory.

**Problem 5.** Let $p$ be a prime number, and $a, b$ be natural numbers. Show that if $p \mid ab$ and $p \nmid a$ then $p \mid b$. (This is Euclid's alternative characterization of prime numbers).

Step 1. Since $p \nmid a$ and $p$ is a prime number, this means that $p, a$ are relatively prime. What can we say about $gcd(a, p)$?

Step 2. Use the result from Step 1 and Theorem 1 to show that we can write 1 as a linear combination of $a, p$.

Step 3. Now, if we want to show that $p \mid b$, how can we use the equation derived from Step 2 to get $b$ on one side without any other terms?

Step 4. Recall that if $p \mid n$ and $p \mid m$ then $p \mid xn + ym$. How can we use this with the fact that $p \mid p$ and $p \mid ab$? Conclude the proof.

**Definition 3.** Let $n$ be a natural number. We say $a$ and $b$ are **congruent modulo n** if there exists an integer $k$ such that $a - b = kn$. In other words, the difference between $a, b$ is divisible by n. We write $a \equiv b \pmod{n}$.

Another way to think about congruence modulo n is if $a$ and $b$ have the same remainder when divided by $n$. Note that by the division algorithm, for any natural number $n$ and integer $a$ there exists a unique $0 \leq r < n$ such that $a \equiv r \pmod{n}$.

**Problem 6.** For the given $a, n$, determine the set of integers that is congruent to $a \pmod{n}$. In other words, find a general form for an integer $x$ such that $x \equiv a \pmod{n}$

1. $a = 0, n = 7$

2. $a = 3, n = 5$

3. $a = -2, n = 12$

4. $a = -8, n = 3$

**Problem 7.** Let n be a natural number. Suppose that $a \equiv b \pmod{n}$. Using Definition 3, show the following:

For any integer $x$, $ax \equiv bx \pmod{n}$

For any integer $y$, $a - y \equiv b - y \pmod{n}$

**Problem 8.** Suppose that $a = qb + r$ where $0 \leq r < b$. Then show that $r \equiv a \pmod{b}$

**Definition 4.** The **multiplicative inverse** of $a$ modulo $n$ is a number $b$ (sometimes denoted $a^{-1}$) such that $ab \equiv 1 \pmod{n}$.

**Problem 9.** Let $a$ be an integer, $n$ be a natural number. When does the multiplicative inverse of $a$ modulo $n$ exist? Prove it. Remember, when $a, n$ are relatively prime, there exists $x, y$ integers such that $ax + ny = 1$. Note that $n \mid ny$. What can we say about $ax \pmod{n}$?

**Problem 10.** Find the multiplicative inverse of $a$ modulo $n$ with the following $a, n$:

1. $a = 13, n = 7$

2. $a = 6, n = 49$

**Problem 11.** Suppose $a$ is an integer, $n$ a natural number and $gcd(a, n) = 1$. How would we use the Extended Euclidean Algorithm along with Theorem 1 to calculate explicitly the number $b$ such that $ab \equiv 1 \pmod{n}$?