BEZOUT'S IDENTITY AND THE EUCLIDEAN ALGORITHM

LIAM DONOVAN

Abstract. We will show one of the most important and well-known results from elementary number theory. We begin by introducing the greatest common factor and then extending our beliefs out to reveal important consequences, in an order that makes such results as obvious as possible.

Contents

Date: April 2023.

1. Euclidean Division

We first must define division. For these examples, we generally examine two integers, a, b. $a \div b$, which can also be written as a/b or as a fraction $\frac{a}{b}$. We define *Euclidean division* as division which only includes integer values. For two integers, a, b there exists a unique q, r, with $b > 0$, such that:

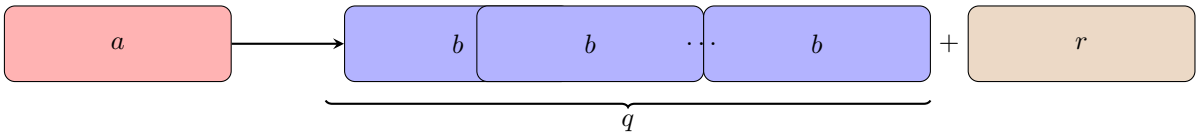
Lemma 1.1 (Euclid's division lemma)**.**

$$a = bq + r \tag{1}$$

where

$$0 \leq r < b$$

This is often called *Euclid's division lemma* or *the division algorithm*[Bur10]. We call q the *quotient* and r the *remainder*. A good analogy to describe this is organizing a objects into groups of b. Once we cannot make another group of b objects, we are left with a number less than b;we cannot make another group, and , if $a = 30$ and $b = 7$, $30 = 7(4) + 2$, since we can make 4 groups of 7, but will have 2 left over.



We now prove the existence and uniqueness.

Proof. If there are a q and r for every a, b then we know that there exists a division statement, in the form above for all a, b. For this we only must show that q or r exists, since the statement above implies that other exists, if one exists. Therefore, we elect to prove the existence of r for all $a, b \in \mathbb{Z}$. Rearranging the division algorithm we can find: $r = a - bq$ and, of course, $r \geq 0$. This means we must prove that the following set is nonempty: $S = \{a - bq : x \in \mathbb{Z}, a - bq \geq 0\}$
We do this by showing that there's a value of q which makes $a - bq$ greater than 0.
Consider if $a \geq 0$:
then we have that, when $q = 0$ $a - b(0) = a \geq 0$ and therefore $a - bq \geq 0$. So, if $a \geq 0$, $a \in S$, thus it is not empty.
Now, consider if $a < 0$:
Since $b \geq 1$ we find that: $-ab \geq -a$ then by adding a: $a - ab \geq 0$. So we can see that this is the division algorithm, if $a = q$. Therefore if $a < 0$, then when $a = q$, $a - qb \in S$, thus S is nonempty. Thus S is nonempty.
Now, we must show that it contains an element, that is less than b, as our condition on r demands. Suppose we have a least element, $r = a - bq^*$. $r \in S$, thus $r \geq 0$. By contradiction, we assume that $r \geq b$

$$\begin{aligned} & r \geq b \\ \implies & a - bq^* \geq b \end{aligned}$$

subtracting b yields:

$$\begin{aligned} a - bq^* - b &\geq 0 \\ a - b(q^* + 1) &\geq 0 \end{aligned}$$

since $q^* \in \mathbb{Z}_+$, $q^* + 1 > q^*$. Thus, because $a \in \mathbb{Z}$, it follows that $a - b(q^* + 1) < a - bq^*$ and so we have found an element of S that is less than the least element, and thus, we find a contradiction. Thus, there exists at least one element in S that is less than b.

Now we move to prove that q, r are unique, for a certain a, b.
Assume there exists two q, r values for which $a = bq + r$ as follows:

$$\begin{aligned} a &= q_1 b + r_1 \\ a &= q_2 b + r_2 \end{aligned}$$

where $0 \leq r_1 < b$, $0 \leq r_2 < b$.

if then $q_1 = q_2$ and $r_1 = r_2$, then there is only one, unique q, r. Without loss of generality assume $r_1 \geq r_2$. By subtracting the top equation from the bottom yields:

$$0 = b(q_1 - q_2) - (r_1 - r_2) \tag{2}$$

$$\implies r_1 - r_2 = b(q_1 - q_2) \tag{3}$$

Since we assume $r_1 \geq r_2$, and $b > 0$, we know $q_1 - q_2 \geq 0$. Thus,

$$\implies r_1 - r_2 \geq b \tag{4}$$

(5)

Then reexamining our initial bounds on r_1, r_2:

$$0 \leq r_2 < r_1 < b$$

Since $r_2, r_1 \in \mathbb{Z}_+$, we conclude that $0 < r_2 - r_1 < r_2$. And because $r_2 < b$, we conclude

$$0 < r_1 - r_2 < b$$

But, this directly contradicts (4). Thus, we find $r_1 - r_2 = 0$. And because

$$r_1 - r_2 = b(q_1 - q_2)$$

$$\implies q_1 - q_2 = 0$$

Since $b > 0$. Then, both of the results for r_1, r_2 and q_1, q_2 are equivalent to:

$$r_1 = r_2$$

$$q_1 = q_2$$

Thus, for a certain a, b, $\exists! q, r$.[Uni] □

We say that b *divides* a if and only if $a = qb$, that is, b can be written as a *factor* of a. In this case, we can see there is no remainder in the division algorithm, for a and b, if $a \geq b$, $r = 0$. In the previously stated analogy, this means that a can be separated into groups of b, with no leftovers, no remainder. We denote this as $b \mid a$. Restated this is:

Definition 1.1 (Divisibility)**.**

$$b \mid a \iff a = bq \tag{6}$$

where $q \in \mathbb{Z}$, $b > 0$.

2. The Greatest Common Divisor

Now, we introduce the idea of the greatest common divisor or the *gcd*. We elect it to be more convenient to write division as a fraction, in these cases. For example: we write $a \div b$ as $\frac{a}{b}$. First, consider the following example:

$$\frac{12120}{80}$$

while this can be computed manually, using long division, one may elect to reduce both numbers to their *prime factorization*:

$$\frac{2^3 \cdot 3^1 \cdot 5^1 \cdot 101^1}{2^4 \cdot 5^1}$$

Then, by the properties of fractions, and exponents, we can rewrite this as:

$$\frac{2^3}{2^3} \cdot \frac{3^1 \cdot 5^1 \cdot 101^1}{2^1 \cdot 5^1}$$

Then, again, using the properties of fractions:

$$\frac{2^3 \cdot 5^1}{2^3 \cdot 5^1} \cdot \frac{3^1 \cdot 101^1}{2^1} = \frac{3^1 \cdot 101^1}{2^1}$$

Note that the proof that a fraction can be reduced to its prime factorization is given by the *fundamental theorem of arithmetic*. It is not needed for further reading within this paper and will be omitted.

Then, since the prime factorization shares no more terms, this is a fully reduced fractions, that is: there's no shared factors, except 1. The common value that must be shared among the numerator and denominator, in order to reduce the fraction fully, is called the *greatest common divisor (gcd)*. Any value that divides both values is called a *common divisor* (the $2^1, 2^2, 2^3, 5^1$), the greatest common divisor is a product of all the common divisors ($2^3 \cdot 5^1$).

The *gcd* is uniquely defined by two properties. First, of course, it is a *factor* of both numbers, i.e., let d be the *gcd* of a, b, $a = ds$ and $b = dt$, where $s, t \in \mathbb{Z}$. Second, because it is a product of all the common divisors, all the common divisors divide the gcd, i.e., let c be any common divisor of a and b, $c \mid d$. We denote the *gcd* of a, b as:

$$gcd(a, b)$$

For convenience, throughout this work, we let $gcd(a, b) = d$.

Note that $gcd(a, b) = gcd(-a, b) = gcd(a, -b) = gcd(-a, -b)$, thus we elect to restrict the *gcd* to the positive case, that is: $gcd(a, b) \in \mathbb{N}$.

We say that if the $gcd(a, b) = 1$, a, b are *coprime*. Since 1 is a factor of all integers, x, $x \cdot 1 = x$ this indicates that there are no common factors in the prime factorization, except the trivial common factor, 1.

Definition 2.1.

$$\text{a,b are coprime} \iff gcd\,(a, b) = 1 \tag{7}$$

Two integers being coprime implies that their fraction cannot be reduced further, i.e., it is an irreducible fraction.[CR13] As previously stated, a gcd is a product of all the common factors of a and b, therefore, dividing by it leaves no common factors in the decomposition, meaning that the remaining fraction is irreducible. That is:

Proposition 2.1. *Let* $gcd(a, b) = d$

$$gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1 \tag{8}$$

Proof. Let $gcd\,(a, b) = d$:
by definition 1.1: $\exists s, t \in \mathbb{Z}$ such that

$$a = ds \tag{9}$$

$$b = dt \tag{10}$$

Rearranging, we obtain: $\frac{a}{d} = s$, $\frac{b}{d} = t$, thus we must prove $gcd\,(s, t) = 1$.
Assume $gcd\,(s, t) \neq 1$: Thus, there must exist some $k \neq 1$ such that $gcd(s, t) = k$. Thus, we can know, by definition 1.1 $\exists m, n \in \mathbb{Z}$ such that $s = km$ and $t = kn$. Plugging into (9), (10) yields:

$$a = d(km)$$

$$b = d(kn)$$

Thus $dk \mid a$ and $dk \mid b$. Since $gcd(s,t) = k \in \mathbb{N} \setminus \{1\}$, it follows:

$$\begin{aligned} & k > 1 \\ \implies & dk > d \end{aligned}$$

which is a contradiction, since it states that there is some common divisor $gcd(a,b) = dk$ which exceeds the $gcd(a,b) = d$. Thus, $gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. □

In addition, we find that the *gcd* of a with any multiple of b, or vice-versa, is equal to the $gcd(a,b)$. That is:

Claim 2.1. $\forall x, y \in \mathbb{Z}$

$$gcd\,(a,b) = gcd\,(a + xb, b) = gcd\,(a, b + ya) \tag{11}$$

First, we must prove a, rather obvious, property of the common divisors.

Lemma 2.1. *Let $a, b, c, d, e \in \mathbb{Z}$. If $c \mid a$ and $c \mid b$ then $c \mid (ad + be)$*

Proof. Since $c \mid a$, $c \mid b$, by definition 1.1 $\exists s, t \in \mathbb{Z}$ such that $a = cs$, $b = ct$. Then we find:

$$\begin{aligned} ad + be &= cs(d) + ct(e) \\ &= c(sd + te) \end{aligned}$$

Thus, $ad + be$ divides c. □

This result is obvious when considering the prime factorization of the a, b. If we add more of the prime factorization of both numbers, then, we are strictly adding factors, so the integers that divided a, b will still divide the sum of the products of a, b. This is called a *linear combination* of a, b.

Proof. Now, to prove the above claim, let $a, b, c \in \mathbb{Z}$. We want to show that all common divisors of a and b are identical to those of $a + xb$ and b. We elect to show the case $gcd\,(a,b) = gcd\,(a + xb, b)$ the alternate case is analogous.

Let $r \in \mathbb{Z}$ be a common divisor of a, b, thus by lemma 2.1: $r \mid a, b$ and $r \mid ax + by$. Letting $x = 1$, we then know $r \mid a + by$. So all the common divisors of a, b are also common divisors of $ax + by$.

Now consider a common divisor of $a + by$ and b, call it f. Then $f \mid a + by$ and $f \mid b$. By lemma 2.1, letting $x = 0$, $y = -1$, we find that $f \mid (a + by) - by = a$. Thus $f \mid a$, also. Therefore, we find that all the common divisors of a, b are identical to the common divisors of $a + xb$ and b. Since the *gcd* is the product of the common divisors, the $gcd(a,b) = gcd(a + bx, b)$. Again, the proof for $gcd(a,b) = gcd(a, b + ay)$ is analogous. □

There exists another apparent result from the *gcd*, which is crucial in elementary number theory. It is stated as follows:

Observation 2.1. Let $x \in \mathbb{Z}$

$$gcd(0, x) = x \tag{12}$$

This is a result of the observation that $\forall x \in \mathbb{Z}$, $x \mid 0$. Since for any integer x, $\frac{0}{x} = 0$, so all integers divide 0. Then, of course, the greatest factor of x is x, so the $gcd(0, x) = x$.

3. The Euclidean Algorithm

Now, we examine a result to compute the *gcd*, by using the results from the properties of the *gcd*. Observe the following from claim 2.1: since $gcd(a,b) = gcd(a, b-ay)$. By use of the division algorithm (lemma 1.1) we find:

$$a = bq + r \implies r = a - bq$$

Thus, by claim 2.1, we know that $gcd(a,b) \mid r$. Formally:

Observation 3.1.

$$gcd(a,b) = gcd(b,r) \tag{13}$$

where r is the remainder of $\frac{a}{b}$.

Proof. By lemma 1.1, we can rewrite:

$$a = bq + r$$

as:

$$r = a - bq$$

which shows that r is a linear combination of a, b, where $-q = y$, in the form of claim 2.1. Therefore, since $gcd(a,b) \mid a, b$ we find that $gcd(a,b) \mid r$. So, the common divisors of a, b are the same as the common divisors of b, r. Thus, we conclude $gcd(b,r) = gcd(a,b)$ □

This indicates that the *gcd* of a dividend and its divisor is equivalent to the *gcd* of the divisor and the remainder.

An application of this idea is as follows:
by repeated application of observation 3.1, we can iterate the division algorithm as follows:

$$a = bq_1 + r_0 \qquad gcd(a,b)$$

then since the $gcd(a,b) = gcd(b,r)$, we can write another Euclidean division, where b is the dividend and r_1 is the divisor, and continue:

$$\begin{aligned} b &= r_0 q_2 + r_1 && gcd(b, r_0) \\ r_0 &= r_1 q_3 + r_2 && gcd(r_0, r_1) \end{aligned}$$

eventually, if $r_n = 0$, we find:

$$\begin{aligned} &\vdots \\ r_{n-2} &= r_{n-1} q_{n+1} && gcd(r_{n-2}, r_{n-1}) \\ r_{n-1} &= 0(q_{n+2}) + r_{n-1} && gcd(r_{n-1}, 0) \end{aligned}$$

Then, we know that $gcd(a,b) = gcd(b,r_1) = \cdots = gcd(r_{n-1}, 0) = r_{n-1}$ by observation 2.1. Thus, the algorithm shows that the *gcd* of a, b is the quotient, when the remainder is 0. This is called the *Euclidean algorithm*. To prove its validity, we must show that r_n is the $gcd(a,b)$ that is: r_n divides both a, b and for all common divisors c, $c \mid r_n$. Then we must show that the remainders eventually go to 0.

Proof. First, confirmation that r_{n-1} is indeed the $gcd(a,b)$. Let $gcd(a,b) = d$. For this r_{n-1} must divide a, b. From the second to last step of the algorithm, we find $r_{n-1} \mid r_{n-2}$. From the third to last step of the algorithm we find $r_{n-3} = r_{n-2} q_{n-1} + r_{n-1}$. Since $r_{n-1} \mid r_{n-2}, r_{n-1}$, and r_{n-3} is a linear combination of r_{n-2} and r_{n-1}, by claim 2.1, $r_{n-1} \mid r_{n-3}$. Since r_{n-4} is a linear combination of r_{n-3} and r_{n-2} $r_{n-1} \mid r_{n-4}$. This continued process validates that r_{n-1} divides all the remainders and quotients in the algorithm, thus $r_{n-1} \mid a, b$. Thus, we know that r_{n-1} is a common divisor of a, b, so $r_{n-1} \leq d$.

In addition, we can see that any common divisor, call it α, of a, b also divides r_k, $\forall k \leq n$, by observation 3.1. And because $\alpha \mid a, b$ we can write: $a = \alpha s$, $b = \alpha t$ for some $s, t \in \mathbb{Z}$. Thus we can see that α divides r_0, since $r_0 = a - bq_1 = \alpha s - \alpha t q_1 = \alpha(s - tq_1)$. For the same reason, $\alpha \mid r_1$, since we can write: $r_1 = b - r_0 q_2 = \alpha t - \alpha s_1 q_2 = \alpha(t - s_1 q_2)$, where $s_1 \in \mathbb{Z}$. So, $\alpha \mid r_1$. This continued process gives: $\alpha \mid r_k$, $\forall k \leq n$. Of course, the $gcd(a,b)$ is a common factor of a, b, thus $gcd(a,b) = d \mid r_k$, in particular, $d \mid r_{n-1}$. Thus, since $d \in \mathbb{N}$, it follows: $d \leq r_{n-1}$.

The result from our two arguments is:

$$d \leq r_{n-1} \leq d$$

Thus, by the squeeze theorem, we find $r_{n-1} = d = gcd(a, b)$. Now, we must prove that r_k eventually goes to 0. Using the assumptions from lemma 1.1:

$$\begin{aligned} 0 \leq r_1 &< b \\ 0 \leq r_2 &< r_1 \\ &\vdots \\ 0 \leq r_n &< r_{n-1} \end{aligned}$$

Thus, $0 \leq r_n \leq r_{n-1} \leq \cdots r_1 \leq r_0 < b$. Noting that $r_k \in \mathbb{N}$, and is strictly decreasing, eventually $r_k = 0$. □

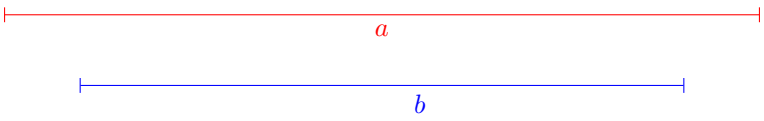
Example. Find $gcd(42, 30)$ using the Euclidean algorithm

$$\begin{aligned} 42 &= 30(1) + 12 \\ 30 &= 12(2) + 6 \\ 12 &= 6(2) + 0 \end{aligned}$$

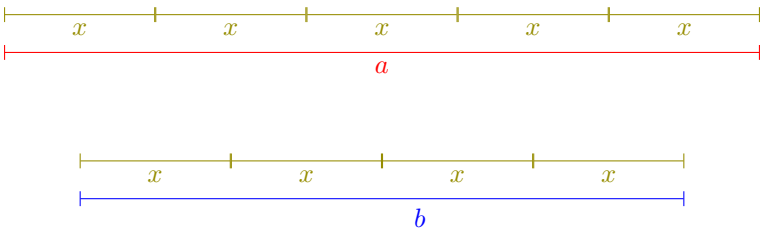
Thus, the $gcd(42, 30) = 6$.

4. Visualization of the Euclidean Algorithm

A visualization of the *gcd* can be shown using string. Consider that we have 2 pieces of string, one of length a, and another of length b.

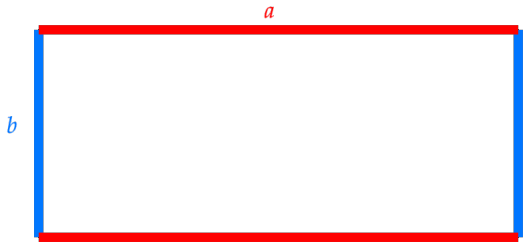


If a, b is divisible by x if we can create a string of length of a, b using strings of length x.[um18] That is:



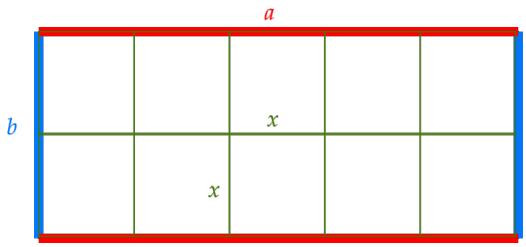
Here, since $b = 4x$ and $a = 5x$, x is a comon factor of a, b. Of course, if there is *overhang*, then $x \nmid a$ and/or $x \nmid b$.

It is more interesting to view this as a rectangle as follows:



[1] Now we may consider common factors of a, b as squares. For example, let x be a common divisor of a, b:

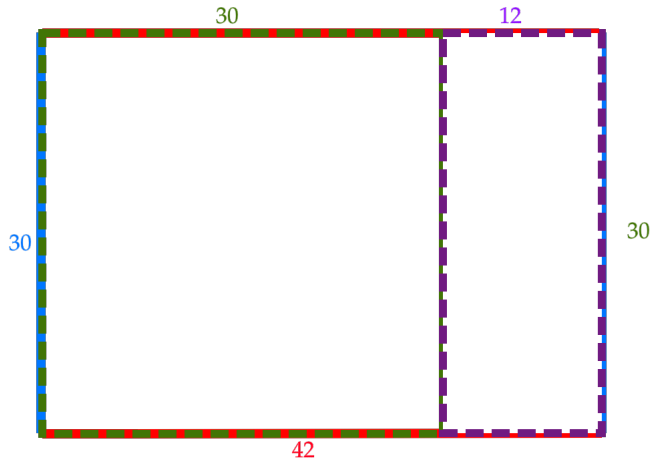
[1]All figures in this section are made by the author, using mathcha and tikz. A link to the figures in mathcha is given: https://www.mathcha.io/editor/2rNWeC79U5DtG6MXXxh0XJmoBf09PPD4CllQ3yd.



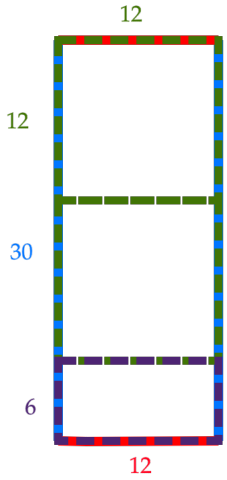
So, the *gcd* is the biggest squares than can fill the rectangle, without any leftover space, or overhang. The Euclidean algorithm explains that we can look at the $a \times b$ rectangle, then create $b \times b$ squares, which will have some leftover, r (unless the rectangle is actually a $a \times a$ square, which is also a b, b square, which implies that b is the *gcd*). We do this until we cannot fit anymore $b \times b$ squares. This is analogous to the first step, where we examine $gcd(a, b)$, by looking at $a = bq_1 + r_0$. Then we look at the $r \times b$ rectangle, which corresponds to examining the $gcd(b, r)$, by looking at $b = r_0q_2 + r_1$. Of course, by claim 2.1, we know that this is equivalent to $gcd(a, b)$. We continue this process until we arrive at $r_{n-2} = r_{n-1}q_{n+1}$, which means there's no leftovers, we can make a $r_{n-2} \times r_{n-1}$ rectangle out of $r_{n-1} \times r_{n-1}$ squares, which means r_{n-1} is the $gcd(a, b)$.

Example. Compute $gcd(42, 30)$ using rectangles.

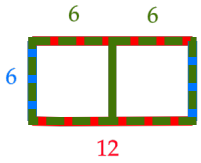
We begin with a 42×30 rectangle. We know then make 30 square, which we can only fit one of.



This represents the step: $42 = 30(1) + 12$, which corresponds to $gcd(42, 30)$. Then we examine the $r \times b$ rectangle, in this case, a 12×30 rectangle (written in purple). We can fit 2 12×12 squares in this.



This is the step: $30 = 12(2) + 6$, which corresponds to $gcd(12, 6)$. Then, again, we examine the rectangle with the side lengths of the remainder and the quotient, in this case, a 12×6 rectangle. We can fit 2 6×6 squares in the rectangle, with no remainder.



This corresponds to $12 = 6(2) + 0$ and $gcd(6, 0) = 6$. Which from claim 2.1 is equal to $gcd(42, 30)$ and thus conclude $gcd(42, 30) = 6$.

5. Bézout's Identity

A consequence of the Euclidean algorithm is as follows:
Consider $r_0 = a - bq_1$, noting that r_0 is a linear combination of a, b. Then performing the next step yields: $r_1 = r_0q_2 + r_1 = (a - bq_1)q_2 + r_1$. Thus, r_1 is also a linear combination of a, b. Repeating this indicates that all r_k are linear combinations, since r_0 is nested within all r_k. Thus, r_{n-1} is also a linear combination of a, b. Since $r_{n-1} = gcd(a, b)$, this motivates the idea that the $gcd(a, b)$ is a linear combination of a, b. That is:

Corollary 5.1 (Bézout's Identity)**.** *$\exists x, y \in \mathbb{Z}$ such that:*

$$ax + by = gcd(a, b) \tag{14}$$

We refer to x, y as *Bézout coefficients* for (a, b). Before we begin the proof, we must state the *well-ordering Principle* for natural numbers.

Axiom (Well-ordering principle)**.** For all nonempty subsets, S, of $\mathbb{N}$ there exists a least element. That is:

$$\forall S \subset \mathbb{N}$$

S has a least element.

The set we are interested in is the set $S = \{ax + by : x, y \in \mathbb{Z},\ ax + by > 0\}$. We want to prove that $gcd(a, b)$ is the least element of S, which trivially exists, by the well-ordering principle.

Proof. First, we prove S to be nonempty. Consider the case where $a > 0$. Then, let $y = 0$, $x = 1$. This results in $a + b(0) = a$. Thus a is in S, thus S is nonempty. If $a < 0$, then we let $y = 0$, $x = -1$, meaning a is once again in S, meaning S is nonempty. Therefore, by the well-ordering principle, S has a least element, we elect to denote it $d = ar + bt$. We now show that the least element is the $gcd(a, b)$. First, we must show that d divides a, b. By lemma 1.1, we find

$$a = dq + r$$

where $0 \leq r < d$

plugging in $d = ar + bt$:

$$\begin{aligned} & a = (ar + bt)q + r \\ \implies\ & r = a - (ar + bt)q \\ & = a(1 - qr) - b(qt) \end{aligned}$$

Thus, r is a linear combination of a, b and so either r is in S or is 0, since $0 \leq r < d$. But, of course, d is the least element in S and $r < d$, so $r \notin S$, which means $r = 0$. Thus, by definition 1.1 $d \mid a$. The proof for $d \mid b$ is analogous to the above case.

Now, it must be shown that d divides all common divisors. Let c be any common divisor of a, b. By definition 1.1, we know $a = \alpha c$, $b = \beta c$ for some $\alpha, \beta \in \mathbb{Z}$. Plugging this into the definition of d yields

$$\begin{aligned} d &= \alpha c(r) + \beta c(t) \\ &= c(\alpha r + \beta t) \end{aligned}$$

Thus, d divides all c, i.e., $d \mid c$. Therefore, $d = gcd(a, b)$ □

Remark 5.1. Since $d = gcd(a, b)$ is the least element of S, the other members of the set are the *multiples* of d that is:

$$\begin{aligned} S &= \{ar + bt,\ 2(ar + bt), 3(ar + bt) \cdots\} \\ &= \{d, 2d, 3d \cdots\} \end{aligned}$$

That is: the integers of the form $ax + by$ are the multiples of the $gcd(a, b)$.

Remark 5.2. Bézout coefficients are trivially not unique[2]. Consider $gcd(3,1) = 1$. The following are all Bézout coefficients:

$$1 = 3(2) + 1(1) \xrightarrow{coef} (2,1)$$
$$1 = 3(1) + 1(-1) \xrightarrow{coef} (3,-1)$$
$$1 = 3(100) + 1(-299) \xrightarrow{coef} (100,-299)$$
$$\vdots$$

[2]We will derive the general form for Bézout coefficients in a future result.

6. The Extended Euclidean Algorithm

The proof for Bézout's identity is said to be non-constructive, in that it only proves existence of x, y, but does not provide a way to find x, y. Performing the Euclidean algorithm finds the $gcd(a, b)$, using a linear combination of a, b, which is the remainder, r_0. Thus, if the process was iterated backwards, starting with the $gcd(a, b)$ we could find a linear combination of a, b.

Example. Find Bézout coefficients for $42, 30$.
We found that $gcd(42, 30) = 6$. We elect to rearrange to solve for 6, since that is our end goal. Rearranging from second to last equation: $6 = 30(1) - 12(2)$. We have $a = 30$, but still lack a $b = 42$, so we return to the first line of the algorithm, by rearranging: $12 = 42 - 30(1)$. Then we plug in: $6 = 30(1) - (42 - 30(1))(2) = 30(3) + 42(-2)$. Thus two Bézout coefficients for $42, 30$ are $-2, 3$, respectively.

The extended Euclidean algorithm is particularly useful when a, b are coprime. In these cases, x is the modular multiplicative inverse of $a \mod b$. That is: $ax \equiv 1 \pmod b$. Likewise for y, it is the modular multiplicative inverse of $b \mod a \implies by \equiv 1 \pmod a$.[Sta13]

7. Connection to Linear Diophantine Equations

We define a linear Diophantine equations as follows:

Definition 7.1. A *linear Diophantine equation* is a sum of two (or more) linear (monomial; degree 1) equations. Often times, this is expressed in terms of x and y:

$$ax + by = c \tag{15}$$

where $a, b, c \in \mathbb{Z}$

Notice that c is a linear combination of a, b, as is the case in Bézout's identity. Thus, we know if $c = gcd(a, b)$, then there are at least 1 solution to the equation. Moreover, we found in remark 5.1 that the multiples of the $gcd(a, b)$ are linear combinations of a, b. That is: there exists a linear combination of a, b for all multiples of $gcd(a, b)$. This motivates the idea that a linear Diophantine equation may have no integer solutions for x, y if c is not some multiple of the $gcd(a, b)$.

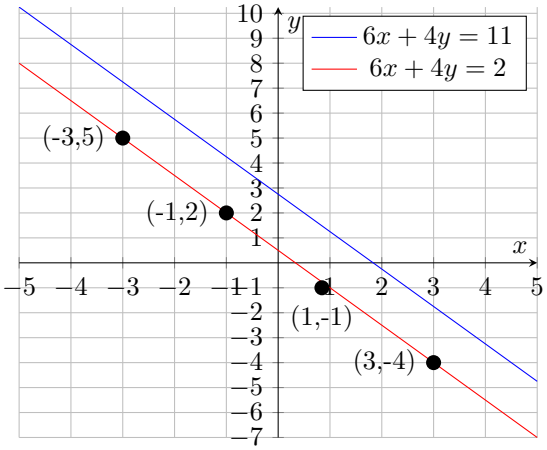
Proposition 7.1. *Let a, b be integers. Let $gcd(a, b) = d$ and k be an arbitrary integer. If $c \neq kd \iff d \nmid c$, then $\nexists x, y \in \mathbb{Z}$ such that $ax+by = c$ then $\nexists x, y \in \mathbb{Z}$ that satisfies the linear Diophantine equation, $ax+by = c$. Inversely, if $d \mid c$, then $\exists x, y \in \mathbb{Z}$ that satisfies the equation.* [Bur]

Proof. By contradiction, assume $\exists x, y = x_0, y_0$ such that $ax_0 + by_0 = c$, where $d \nmid c$. By definition 1.1, $\exists r, t \in \mathbb{Z}$ such that $a = dr$ and $b = dt$. Plugging these into the linear equation yields:

$$(dr)x_0 + (dt)y_0 = c$$
$$d(rx_0 + ty_0) = c$$

But this implies that $d \mid c$, which contradicts our assumption, thus the statement is false.
By corollary 5.1, we know the inverse to be true. □

Example. A common way to express linear Diophantine equations is as lines in the Euclidean plane, hence its name. For example: consider $6x + 4y = 11$ and $6x + 4y = 2$:



[3] Notice that, since $gcd(6,4) = 2$ and $2 \nmid 11$, the line $6x + 4y = 11$ does not intersect any lattice points, i.e., the points where integers x, y meet. Conversely, because $2 \mid 4$, $6x + 4y = 2$ has several points with integer solutions. Rearranging the equations yields $y = \frac{11}{4} - \frac{3}{2}x$.

We can show this equation has no integer solutions.
Assume there exists some solution $x_0, y_0 \in \mathbb{Z}$. Then, $y_0 = \frac{11}{4} - \frac{3}{2}x_0 = \frac{11-6x_0}{4}$. We now must examine if $4 \mid 11 - 6x_0$ for any integer x_0, if so then we have found an integer solution for y_0. Note that $11 - 6x_0$ is the difference of the an even and odd number, which is odd.[Hea81][4] Thus, since $2 \mid 4$, if $11 - 6x_0$ divides 4, it must also divide 2, since 2 is a common divisor. That is: it must be even. But, of course, it is an odd number, therefore our initial assumption was false, so $\nexists x_0, y_0 \in \mathbb{Z}$ such that $4 \mid 11 - 6x_0$. Thus, the linear Diophantine equation $6x + 4y = 11$ does not have an integer solution, as expected.

Of course, since $2 = gcd(6,4) \mid 4$, there do exist integer solutions for $6x + 4y = 2$, as we can find by inspection on the above graph.

Moreover, we can generalize the results for Bézout coefficients. Let c be some multiple of $gcd(a,b)$, then we may rearrange the linear Diophantine equation as: $y = -\frac{a}{b}x + \frac{c}{b}$. Thus, if given an initial point, if x is changed by 1, y experiences a change of $-\frac{a}{b}$. That is: for a change of b in x, there is a change of $-a$ in y, or vice-versa. Given some solution, which must exist by proposition 7.1, (x_0, y_0), we find that another solution exists at $(x_0 - b, y_0 + a)$, since, for a change of b in x, there is a change of $-y$in y. In fact, there will be a solution for all at all points that follow this equation, so, adding factors of a, b can be done many times. Since each new point is the 'new' initial point for the next. Therefore, $(x_0 - nb, y_0 + na)$, where $n \in \mathbb{Z}$. It is not required that $\frac{a}{b}$ be in simplest form, thus we can generalize further, by reducing the fraction to its lowest term. This is done by dividing by the $gcd(a,b)$, by proposition 2.1. Thus, the general form is: $\left(x_0 - n\frac{b}{gcd(a,b)}, y_0 + n\frac{a}{gcd(a,b)}\right)$.

Corollary 7.1. *Let a, b be integers, with $gcd(a,b) = d$. Let $c \mid d$ For all integers, k, the Bézout coefficients of $ax + by = c$ are given by:*

$$\left(x_0 - n\frac{b}{d}, y_0 + n\frac{a}{d}\right) \tag{16}$$

where n is an integer.

Proof. By corollary 5.1 we must show:

$$a\left(x_0 - n\frac{b}{d}\right) + b\left(y_0 + n\frac{a}{d}\right) = d$$

$\forall n \in \mathbb{Z}$

by corollary 5.1, there exists x_0, y_0 such that $ax_0 + by_0 = d$, thus, by the distributive property, we obtain:

$$\begin{aligned}(ax_0 + by_0) - an\frac{b}{d} + bn\frac{a}{d} &= d\\ d - an\frac{b}{d} + bn\frac{a}{d} &= d\end{aligned}$$

by subtracting d

$$\begin{aligned}-an\frac{b}{d} + bn\frac{a}{d} &= 0\\ n\left(-\frac{ab}{d} + \frac{ab}{d}\right) &= 0\\ n(0) &= 0\end{aligned}$$

Thus, $\forall n \in \mathbb{Z}$ the Bézout coefficients are $\left(x_0 - n\frac{b}{d}, y_0 + n\frac{a}{d}\right)$. □

[3] Figure made by the author, using tikz.
[4] The proof is not given here, as it is unrelated to the material of the document.

8. Applications

As previously stated, the extended Euclidean algorithm is useful for when two integers are coprime, since the Bézout coefficients will be the modular multiplicative inverse of $a \mod b$ and $b \mod a$. The extended Euclidean algorithm is used twice in the key generation process in the RSA cryptosystem, once to compute the least common multiple (lcm), defined to be $lcm(a, b) = \frac{|ab|}{gcd(a,b)}$. Then it is used again to find the modular multiplicative inverse.

Bézout's identity can be used to prove both Euclid's lemma, which explains the divisibility of prime numbers. It also can be used to prove the Chinese remainder theorem, which can be used to find the the remainder of an integer n, with the product two integers, ab if we know it's remainder with a and b. For this reason, Bézout's identity is also known as Bézout's lemma.

The Euclidean algorithm is, of course, to motivate Bézout's identity, as well as simplify fractions, as previously stated. It can be used to prove several number theory results, such as the fundamental theorem of arithmetic (unique prime factorization). As we also found, it can be used to prove results for linear Diophantine equations.

Being a basic number theory result, both the Euclidean algorithm and Bézout's identity addresses topics generally covered in elementary schools, thus most students are familiar with the *content*, but not the rigour or implications resulting from these results. This gives it a very low barrier for entry, yet also offers excitement in the discovery of new mathematics.

Additionally, algorithms, in general, are great ways to introduce and motivate topics in computer science, such as efficiency.

Overall, Euclidean algorithm and Bézout's identity are natural ways to introduce the vast landscape of number theory, even to students who are not interested in pure mathematics.

References

[Bur] Burger. The euclidean algorithm and diophantine equations.
[Bur10] David M. Burton. *Elementary number theory*. McGraw-Hill, Higher Education, Boston, 7th edition edition, 2010.
[CR13] Al Cuoco and Joseph J. Rotman. *Learning modern algebra*. MAA Textbooks. Mathematical Association of America, Washington, DC, 2013.
[Hea81] Thomas Heath. *A history of Greek mathematics. Vol. II*. Dover Publications, Inc., New York, 1981. From Aristarchus to Diophantus, Corrected reprint of the 1921 original.
[Sta13] William Stallings. *Cryptography and Network Security: Principles and Practice*. 2013.
[um18] user: mtanti. Finding the greatest common divisor (gcd) / highest common factor (hcf) of two numbers, Feb 2018.
[Uni] Trinity University. The division algorithm.