The Euclidean Algorithm

Abstract

In this session, we shall explore *The Euclidean Algorithm* and related topics. First, we introduce some basic notions of number theory, including the definition of *greatest common divisor* or *gcd*. We shall present the algorithm itself, both with concrete examples as well as in abstract generality. We then use the algorithm to develop some theory, most fundamentally *Bézout's Identity* and its corollaries.

1 Warmup

Exercises:

1.1 What is the smallest positive integer ℓ of the form $7x+11y$, where x and y are integers? (Here, we allow x and y to be positive, negative, or 0.)

1.2 What is the smallest positive integer ℓ of the form $14x+22y$, where x and y are integers?

1.3 What is the smallest positive integer ℓ of the form $6x+10y+15z$, where x, y, z are each integers?

1.4 What is the smallest positive integer ℓ of the form $67x+131y$, where x and y are integers?

Bonus challenge problem: What are *all* pairs of integers (x, y) such that $67x + 131y = \ell$? Try to make a conjecture, even if you can't (yet!) prove it.

2 Introduction: Preliminary Concepts

Before we can jump into our primary topic, let us begin by setting some foundation.

Definition 2.1. Let a, b be integers. Then we say *a divides*[1] b if and only if there is an integer c such that $ac = b$. We denote this by $a \mid b$, read "a divides b". If a, b are integers and a does not divide b, we denote this as $a \nmid b$, read "a does not divide b".

Example 2.2. We have that $2 \mid -6$ because $2, -6$ are integers, $2 \cdot (-3) = -6$, and the quotient -3 is also an integer.

Example 2.3. We have that $3 \nmid 17$ because there is no *integer* c such that $3c = 17$.

Example 2.4. For *every* integer a, $a \mid 0$. This is because $a \cdot 0 = 0$ for all a, and 0 is also an integer.

Conversely, if b is an integer, then $0 \mid b$ if and only if $b = 0$. This is because if there is some integer c such that $0 \cdot c = b$, then we must have $b = 0$.

Remark. Intuitively, if a, b are integers, then $a \mid b$ precisely when either (i) b/a is an integer, or $a = b = 0$ (in which case b/a is undefined).

We can now define a prime number relative to our definition of divisibility:

Definition 2.5. Let p be an integer. Then we say that p is a *prime number* if and only if $p \neq 0$, $p \neq \pm 1$, and whenever a is an integer such that $a \mid p$, then $a = \pm 1$ or $a = \pm p$.

That is, a prime number is neither 0, 1, nor -1, and its only divisors are the "obvious" ones: ± 1 and $\pm p$.

Remark. There are technical reasons to insist that for a prime integer p, $p \neq 0, \pm 1$. In particular, if 1 were considered prime, this would violate the uniqueness provision of The Fundamental Theorem of Arithmetic: every positive integer $n > 1$ is expressible as a product of primes, and in a unique way up to the ordering of the prime factors of n. (After all, $n = n \cdot 1 = n \cdot 1 \cdot 1 = \ldots$, meaning we can include as many factors of 1 in a factorization of n.)

[1] Equivalently: we say a is a *divisor* of b, a is a *factor* of b, or b is a *multiple* of a. (Note the order-reversal of a and b in the final sentence!)

Definition 2.6. Let a, b be integers. Then an integer d is a *common divisor* of a and b if and only if $d \mid a$ and $d \mid b$.

Definition 2.7 (Greatest Common Divisor Definition #1, via Ordering)**.** Let a, b be integers. If at least one of a, b is nonzero, and if d is the largest common divisor of a and b, we say d is the *greatest common divisor* of a and b, denoted $\gcd(a, b)$. If $a = b = 0$, we define $\gcd(0,0) := 0$.

Question: How might you use the above to define $\gcd(a, b, c)$ for three integers?

Definition 2.8. Let a, b be integers. We say that a and b are *relatively prime* or *coprime* if and only if $\gcd(a, b) = 1$.

If a, b are positive integers with $b \neq 0$, then a and b are relatively prime if and only if the rational number a/b is in lowest terms.

Example 2.9. *Claim: Using Definition 2.7,*[2] $\gcd(4,6) = 2$.

To see this, the set of divisors of 4 is precisely $\{-4, -2, -1, 1, 2, 4\}$. Similarly, the set of divisors of 6 is precisely $\{-6, -3, -2, -1, 1, 2, 3, 6\}$. The set of common divisors is thus $\{-2, -1, 1, 2\}$, and the largest of these common divisors is 2. Therefore, $\gcd(4,6) = 2$.

Example 2.10. *Claim:* Using Definition 2.7, $\gcd(-5, 17) = 1$.

Here, we have that the set of divisors of -5 is precisely $\{\pm 1, \pm 5\}$. Similarly, the set of divisors of 17 is precisely $\{\pm 1, \pm 17\}$. The set of common divisors is thus $\{\pm 1\}$, the largest element of which is 1. Therefore, $\gcd(-5, 17) = 1$.

Next is a tool that can help establish prove—or disprove—divisibility, and its theoretical consequences are vast:

Theorem 2.11 (The Division Algorithm)**.** *Let a, b be integers with $b \neq 0$. Then there exist unique integers q, r such that*

$$a = bq + r, \text{ and } 0 \leq r < |b|. \tag{2.1}$$

That is, if a, b are integers and b is nonzero, we can divide a by b to obtain a unique quotient q and nonnegative remainder r such that r is strictly *smaller than $|b|$.*

Remark. The content of Theorem 2.11 is also called *Euclidean Division* or *division with remainder.*

Example 2.12. Consider the case $a := 7$, $b := 3$. Then

$$7 = 3 \cdot 2 + 1, \text{ with } 0 \leq 1 < |3| = 3$$

is the result of (2.1). That is, for $a := 7$, $b := 3$, we have that $q := 2$, $r := 1$ is the unique pair of integers such that $a = bq + r$ and $0 \leq r < |b|$.

[2] We emphasize this distinction because there will later be an alternate—but equivalent—definition of gcd.

Example 2.13. Consider the case $a := 12$, $b := -3$. Then

$$12 = (-3) \cdot (-4) + 0$$

is the result of (2.1). That is, for $a := 12$, $b := -3$, our quotient q is -4, and our remainder r is 0.

Exercises:

2.1 Which of the following statements is true? Explain.

(a) $4 \mid 8$

(b) $5 \mid 13$

(c) $-7 \mid -21$

(d) $18|6$

2.2 For the following integers a, b, compute the corresponding unique q, r such that (2.1) holds.

(a) $a := 17$, $b := 7$.

(b) $a := 19$, $b := -8$.

(c) $a := n+1$, $b := n$, where $n > 1$ is a positive integer. (What happens in the case $n = 1$?)

2.3 Prove the following properties of divisibility.

(a) For every integer n, $n \mid n$. That is, divisibility is *reflexive*.

(b) Let a, b, c be integers such that $a \mid b$ and $b \mid c$. Prove that $a \mid c$.

(c) Let a, b, c be integers such that $a \mid b$ and $a \mid c$. Prove that $a \mid (b + c)$.

(d) Let a, b be *positive* integers. Prove that if $a \mid b$, then $a \leq b$.

(e) Let a, b be *positive* integers. Prove that if $a \mid b$ and $b \mid a$, then $a = b$. That is, for *positive* a and b, divisibility is *antisymmetric*.

Followup: Can you generalize to the case where a, b need not both be positive?

2.4 Prove that if a, b are integers with $b \neq 0$, and $a = bq + r$ as in (2.1), then $b \mid a$ if and only if $r = 0$.

That is, for nonzero b, b divides a if and only if the remainder when dividing a by b is 0.

Remark. Given integers a, b with $b \neq 0$, this result gives a strategy for proving whether $b \mid a$. Namely: consider the remainder r when dividing a by b, and determine whether $r = 0$.

2.5 Let a, b be integers with $a, b \geq 2$. Explain how to compute $\gcd(a, b)$ in terms of the the prime factorizations of a and b.

For example, say that

$$a := 2^{30} \cdot 3^2 \cdot 7^2 \cdot 13^4$$
$$b := 2^2 \cdot 5^2 \cdot 11 \cdot 13.$$

Without multiplying out either number, how can you compute $\gcd a, b$?

2.6 For integers a, b, how would you define the *least common multiple* of a and b? (Notation: $\text{lcm}[a, b]$.) What is $\text{lcm}[4, 6]$? What about $\text{lcm}[3, 17]$?

2.7 Let a, b be integers. If q, r are integers such that $a = bq + r$, prove that $\gcd(a, b) = gcd(b, r)$.

Note: Here q, r are *any* integers such that $a = bq + r$. We need not have that r is minimal in the sense of the Division algorithm.

3 The Euclidean Algorithm

Let us begin by repeating the result, a prelude to the Euclidean Algorithm:

Lemma 3.1. *Let a, b be integers. If q, r are integers such that $a = bq + r$, then*

$$\gcd(a, b) = \gcd(b, r). \tag{3.1}$$

This lemma will be the building block for you to prove the following theorem:

Theorem 3.2 (The Euclidean Algorithm)**.** *Let a, b be integers with $b \neq 0$. Let q_j, r_j be the unique quotients and remainders under the Division Algorithm such that*

$$\begin{aligned}
a &= bq_1 + r_1, && \textit{with } 0 < r_1 < |b| && (3.2)\\
b &= r_1 q_2 + r_2, && \textit{with } 0 < r_2 < r_1 && (3.3)\\
r_1 &= r_2 q_3 + r_3, && \textit{with } 0 < r_3 < r_2 && (3.4)\\
\vdots &\quad\ \vdots && && \\
r_j &= r_{j+1} q_{j+2} + r_{j+2}, && \textit{with } 0 < r_{j+2} < r_{j+1} && (3.5)\\
\vdots &\quad\ \vdots && && \\
r_{n-2} &= r_{n-1} q_n + r_n, && \textit{with } 0 < r_n < r_{n-1} && (3.6)\\
r_{n-1} &= r_n q_{n+1}; && && (3.7)
\end{aligned}$$

that is, n and r_n are defined so that r_n last nonzero remainder from successive applications of the Division Algorithm. Then

$$\gcd(a,b) = r_n; \tag{3.8}$$

i.e., $\gcd(a,b)$ *is this final nonzero remainder.*

What's going on here? For a, b, we Iterate the process of the Division Algorithm, and this eventually returns $\gcd(a,b)$.

First, we divide a by b, then take its remainder r_1; this is the meaning of (3.2). Next, then divide b by the first remainder, r_1, and we take its remainder r_2, as in (3.3). We keep repeating this process in (3.4), dividing r_1 by r_2, forming a remainder r_3; the general recursive step is given by (3.5). Continuing, the final *nonzero* remainder is r_n, in (3.6), and r_n divides the penultimate nonzero remainder r_{n-1} in (3.7). The Euclidean Algorithm tells us that last nonzero remainder, r_n ,is the gcd of our two original integers a and b.

Example 3.3. Apply Euclid's Algorithm to compute $\gcd(47,17)$.

We have

$$\begin{aligned}
47 &= 17\cdot 2+13, && \text{and } 0<13<17\\
17 &= 13\cdot 1+4, && \text{and } 0<4<13\\
13 &= 4\cdot 3+1, && \text{and } 0<1<4\\
4 &= 1\cdot 4.
\end{aligned}$$

Since $r_3 = 1$ is the last nonzero remainder, we conclude that $\gcd(47,17) = 1$.

Exercises:

3.1 Using the Euclidean Algorithm, compute the following greatest common divisors.

(a) gcd(29.11)

(b) $\gcd(731,153)$

3.2 Using the Euclidean Algorithm, reduce the fraction $\frac{741}{637}$ to lowest terms.

3.3 We now prove that the Euclidean Algorithm yields the greatest common divisor.

(a) Prove that the Euclidean Algorithm terminates. That is, prove that we can't continue the chain of equations (3.2)–(3.6) indefinitely with infinitely many nonzero remainders.

(b) Prove that $\gcd(a,b) = \gcd(b, r_1)$

(c) To simplify our general notation, define

$$\begin{aligned} r_{-1} &:= a \\ r_0 &:= b. \end{aligned}$$

Prove that for all nonnegative integers j, $\gcd(r_{j-1}, r_j) = \gcd(r_j, r_{j+1})$.

(d) Prove that $\gcd(a,b) = r_n$.

3.4 The *Fibonacci Sequence*[3] is the sequence $(F_n) = F_1, F_2, F_3, \ldots$ defined recursively via

$$F_1 := 1 \tag{3.9}$$

$$F_2 := 1 \tag{3.10}$$

$$F_{n+2} := F_{n+1} + F_n \text{ for all } n \geq 1. \tag{3.11}$$

The sequence begins $1, 1, 2, 3, 5, 8, 13, \ldots$, continuing infinitely.

Prove that for every positive integer n, $\gcd(F_n, F_{n+1}) = 1$. That is, prove that any two consecutive Fibonacci numbers are relatively prime.

Remark. We can actually say something much stronger: The Fibonacci Sequence is a *strong divisibility sequence*. That is, for all positive integers m, n,

$$\gcd(F_m, F_n) = F_{\gcd(m,n)}.$$

In particular, $F_m \mid F_n$ if and only if $m \mid n$.

4 Linear Combinations and Bézout's Identity

First, a definition:

Definition 4.1. Let a, b be integers. Then a *linear combination* of a and b is an expression of the form $ax + by$, where x, y are also integers.

In particular, for every a, b, a and b are each linear combinations of a and b: $a = a\cdot 1 + b\cdot 0$, and $b = a \cdot 0 + b \cdot 1$.

For a given pair of integers (a, b), we will be especially interested in the following questions:

- Given a, b, can we completely characterize the set of all linear combinations of a and b?

  In particular, if at least one of a and b is nonzero, can we determine the smallest *positive* linear combination of a and b?

[3] *Note:* The advanced group of Chapel Hill Math Circle did a two session exploration of The Fibonacci Sequence on February 11 and February 25, 2023.

- Going in the other direction, if we know that some integer c is a linear combination of a and b, can we produce integers x and y such that $ax + by = c$?

  Further, can we determine the set of *all* integers x, y such that $ax + by = c$?

Our most important goal is to prove *Bézout's Identity* and some corollaries thereto:

Theorem 4.2 (Bézout's Identity)**.** *Let a, b be integers. Then there exist integers x, y such that*

$$ax + by = \gcd(a, b). \tag{4.1}$$

This should be familiar: compare the above goals to the warmup exercises in Section 1.

Exercises:

4.1 In this exercise, we shall see that Bézout's Identity is a consequence of the Euclidean Algorithm

(a) Prove that for a, b, r_j as in (3.2)–(3.7), r_n is a linear combination of r_{n-1} and r_{n-2}. That is, prove that there exist integers x_1, y_1 such that

$$r_n = r_{n-1}x_1 + r_{n-1}x_2. \tag{4.2}$$

(b) For all integers $j \geq -1$, r_{j+1} is a linear combination of r_j and r_{j-1}.

That is, each remainder is a linear combination of the *previous* two remainders.

(c) For all integers $j \geq -1$, r_{j+2} is a linear combination of r_{j+1} and r_j.

That is, each remainder is a linear combination of the *next* two remainders.

(d) Let a, b, c, d, m be integers. Prove that if m is a combination of c and d, and if c and d are each linear combinations of a and b, then m is a linear combination of a and b.

(e) Prove Bézout's Identity holds. That is, prove that $\gcd(a, b)$ is a linear combination of a and b.

4.2 Using Euclid's Algorithm, find integers x, y such that $5x + 3y = \gcd(5, 3)$.

4.3 Let a, b, c be integers such that $a \mid bc$ and $\gcd(a, b) = 1$. Prove that $a \mid c$.

Remark. This is a fundamental property of prime numbers, one not simply an immediate consequence of the definition of prime. By definition, a number is prime based on *its* divisors. Here, a number is prime based on numbers *that it divides.*

4.4 Let a, b, p be integers, with p prime. If $p \mid ab$, prove that $p \mid a$ or $p \mid b$.

Equivalently: assume a, b, p are integers, p is prime, and $p \mid ab$. Prove that if $p \nmid a$, then $p \mid b$.

4.5 Let a, b be integers. Prove that c is a linear combination of a and b if and only if $\gcd(a, b) \mid c$.

References

[1] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers.* Oxford University Press, Walton Street, Oxford OX2 6DP, fifth edition, 1979.

[2] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An Introduction to the Theory of Numbers.* John Wiley & Sons, Inc., New York, fifth edition, 1991.