# Euclidean Algorithm I

BMC Fall 2019

September 21, 2019

## 1 Divisors

**Definition 1.1.** *For integers $k, n \in \mathbb{Z}$, we say that $k$ is a* ***factor or divisor*** *of $n$ if $n/k$ is an integer. In this case, we write $k \mid n$, which is read as "$k$ divides $n$."*

**Example 1.2.** *The positive divisors of* $18$ *are* $1, 2, 3, 6, 18$.

**Exercise 1.3.** *List all the positive factors of* $12$ *and* $20$.

**Exercise 1.4.** *What are the divisors of* $0$*?*

**Definition 1.5.** *Let $a, b \in Z$ be integers that are both non zero. The* ***greatest common divisor (gcd)*** *of $a, b$ is the largest integer $d$ that is a divisor of both $a$ and $b$. We write that $d = \gcd(a, b)$ or $d = (a, b)$.*

**Example 1.6.** *What is the gcd of* $12$ *and* $20$*?*

**Exercise 1.7.** *What is $(7, 7)$? What about $(n, n)$ for some $n \geq 1$?*

**Exercise 1.8.** *What is $(6, 18)$? $(5, 15)$? What about $(n, 3n)$ for some $n \geq 1$?*

**Exercise 1.9.** *What is $(n, 0)$ for some $n \geq 1$? Why did we say we can't take the gcd of $0$ with itself?*

## 2 Division Algorithm

**Theorem 2.1** (Division Algorithm)**.** *Given two integers $a, b \in \mathbb{Z}$ with $b > 0$, there exist unique integers $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < q$. We call $r$ the* ***remainder*** *when we divide $a$ by $b$.*

**Example 2.2.** *When dividing $236$ by $55$, we get that $236 = 55 \cdot 4 + 16$ so $q = 4$ and $r = 16$. For our purposes, we will really only be interested in the remainder $r$.*

**Exercise 2.3.** *Find the remainder when we divide $254$ by $32$. Find the remainder when we divide $407$ by $74$.*

**Exercise 2.4.** *Show that if $d$ is a divisor of both $a, b$, then $d$ is also a divisor of $r$. Vice versa show that if $d$ divides both $b, r$, then $d$ is a divisor of $a$.*

**Exercise 2.5.** *Use the previous exercise to prove that $(a, b) = (r, b)$.*

# 3 Euclidean Algorithm

**Exercise 3.1.** *Consider the following calculation:*

$$236 = 4 \cdot 55 + 16 \tag{1}$$
$$55 = 3 \cdot 16 + 7 \tag{2}$$
$$16 = 2 \cdot 7 + 2 \tag{3}$$
$$7 = 3 \cdot 2 + 1 \tag{4}$$
$$2 = 2 \cdot 1 + 0. \tag{5}$$

*What is going on and how does it relate to the fact that*

$$(236, 55) = (55, 16) = (16, 7) = (7, 2) = (2, 1) = (1, 0) = 1.?$$

**Exercise 3.2.** *Describe in words how the Euclidean algorithm works. Then use it to find the gcd of* $(254, 32), (407, 74)$ *and* $(270, 192)$.

**Exercise 3.3.** *Use the calculations in Exercise 3.1 to write* $16$ *as a linear combination of* $236$ *and* $55$ *(write* $16 = 236 \cdot x + 55 \cdot y$*). Then write* $7$ *as a combination of* $55$ *and* $16$*. Use the previous part to substitute* $16$ *to get* $7$ *as a combination of* $236$ *and* $55$.

**Exercise 3.4.** *Repeat the previous calculations until you write* $1$ *as a linear combination of* $236$ *and* $55$.

**Exercise 3.5.** *Repeat the same process to write* $(254, 32)$ *as a linear combination of* $254$ *and* $32$*. Do the same for* $(407, 74)$ *and* $(270, 192)$.

**Theorem 3.6** (Bezout's Theorem)**.** *For any two integers $a, b \in \mathbb{Z}$ not both zero, there exist integers $x, y$ such that $ax + by = g = (a, b)$.*

**Exercise 3.7.** *Are the integers $x, y$ unique? e.g. when we write* $236 \cdot (-24) + 55 \cdot (-103) = 1$*, are there any other choices other than $x = -24$ and $y = -103$ that make this true?*

**Theorem 3.8** (Euclid's Lemma)**.** *If $d \mid ab$ and $(d, a) = 1$, then $d \mid b$.*

**Example 3.9.** *We can use Euclid's Lemma to help us quickly determine if a number is divisible by another. We can use this to determine if* $2027$ *is divisible by* $17$.

**Exercise 3.10.** *Is* $7544$ *divisible by* $23$*? Is* $3636$ *divisible by* $13$*? Is* $5410$ *divisible by* $21$*?*

**Exercise 3.11.** *Find a counter example to Euclid's lemma if $(d, a) \neq 1$.*

# 4 Unique Prime Factorization

**Definition 4.1.** *A* ***prime number*** *is a positive number with only two positive divisors:* 1 *and itself. Any positive number that is not prime is called* ***composite****.*

**Exercise 4.2.** *What are the possible values for* $(p, n)$ *for some prime* $p$ *and some integer* $n \in \mathbb{Z}$*.*

**Lemma 4.3.** *If* $p$ *is a prime number and* $p \mid ab$*, then* $p \mid a$ *or* $p \mid b$*.*

**Corollary 4.4.** *If* $p$ *is a prime number and* $p$ *divides a product* $a_1 \cdots a_k$*, then* $p$ *must divide at least one of the* $a_i$*.*

**Lemma 4.5.** *Every integer greater than* 1 *has at least one prime divisor.*

**Theorem 4.6.** *There are an infinite number of primes.*

**Definition 4.7.** *A* ***twin prime*** *is a pair of primes that differ by* 2*, so* $p$ *and* $p + 2$*.*

**Conjecture 4.8** (Twin Prime Conjecture)**.** *There are an infinite number of twin primes.*

**Exercise 4.9.** *Prove that* 5 *is the only prime that is part of two twin primes.*

**Conjecture 4.10** (Goldbach's Conjecture)**.** *Every even integer greater than* 2 *can be written as the sum of two primes.*

**Theorem 4.11.** *Every positive integer greater than* 1 *can be uniquely written as a product of primes.*

**Exercise 4.12.** *What is the prime factorization of* 63*? What about* 48*?*

**Exercise 4.13.** *Prove that any composite number* $n$ *must have a prime divisor* $p$ *that satisfies* $p \leq \sqrt{n}$*.*

Problems are adapted from a worksheet on the Euclidean Algorithm by Professor Karen E. Smith of the University of Michigan.