Divisibility

Written by Dmitry Badziahin and Andy Tran for the MaPS Program

1 Introduction

The study of integers, called **Number Theory**, is one of the oldest branches of mathematics and has been of interest to humans dating back to Ancient Mesopotamia, Egypt, Greece, India and so on. One fundamental concept that separates integers from other numbers is the idea of **divisibility**. This seemingly basic idea has far reaching implications that builds the entire field of Number Theory.

This topic will introduce the core definitions of divisibility and extend this to the **Fundamental Theorem of Arithmetic**, the **Euclidean Algorithm** and **Bézout's Identity**.

2 Notation

To start off, let's introduce some notation.

- We say that an integer a **divides** an integer b if there exists some other integer k such that $b = ak$.
- We could equivalently say that "b is a **multiple** of a" or "b is **divisible** by a". Or we could say that "a is a **factor** of b" or "a is a **divisor** of b".
- Mathematically, we will write $a|b$ which can be read out as "a **divides** b".
- A number $p > 1$ is a **prime** if its positive divisors are only 1 and itself.
- If we have that $p^k|n$ and $p^{k+1} \nmid n$, we say that p^k is the **highest prime power** of p that divides n and we denote this by $p^k \parallel n$. This can also be written as $\nu_p(n) = k$.
- A final piece of notation is that we will use $\in$ to mean "**in**" and $\mathbb{Z}$ to denote "**the set of integers**". So the mathematical expression $n \in \mathbb{Z}$ is a concise way of saying that "n is **in** the **set of integers**" or we could read this out as "n **is an integer**". Below is a list of commonly used sets in mathematics

Symbol	Set
$\mathbb{Z}$ or $\mathbb{J}$	Integers
$\mathbb{Z}^+$	Positive Integers
$\mathbb{Z}_0^+$	Non-negative Integers
$\mathbb{N}$	Naturals (sometimes controversial)
$\mathbb{Q}$	Rationals
$\mathbb{R}$	Reals
$\mathbb{C}$	Complex Numbers

Exercise 2.1 *Why are the natural numbers "controversial"?*

3 Divisibility

We can now look at the key properties of divisibility!

(1) For $a, b, c \in \mathbb{Z}$, if $a \mid b$ then $a \mid bc$

(2) For $a, b, c \in \mathbb{Z}$, if $a \mid b$ and $b \mid c$ then $a \mid c$

(3) For $a, b, c \in \mathbb{Z}$, if $a \mid b$ and $a \mid c$ then $a \mid b + c$

These properties may seem obvious, but they can be proven rigorously, that is using the definition of divisibility. Consider the following example:

Example 3.1 *Prove that for $a, b, c \in \mathbb{Z}$, if $a|b$ then $a|bc$.*

Recall that the definition of a dividing b means that there exists some integer k such that $b = ak$. Hence, we may say:

$$\begin{aligned} a \mid b &\implies b = ak \text{ for some } k \in \mathbb{Z} \\ &\implies bc = akc \\ &\implies bc = a(kc) \\ &\implies a \mid bc \text{ because } kc \in \mathbb{Z} \end{aligned}$$

□

Exercise 3.2 *Prove the other two properties.*

Another crucial property about divisibility has to do with primes and is given its own special name!

Theorem 3.3 (Euclid's Lemma) *For a **prime** p and integers a, b, if $p \mid ab$ then $p \mid a$ or $p \mid b$*

These seemingly basic properties can actually be used to prove some powerful mathematical results! Consider these examples.

Example 3.4 *For integers m, n, prove that $17 \mid 2m + 3n$ if and only if $17 \mid 3m - 4n$.*

Notice that we have an "if and only if" statement, which means that we need to prove **two implications**! However, we can address this elegantly by only using **two-way arguments**.

$$\begin{aligned} 17 \mid 2m + 3n &\iff 17 \mid 3(2m + 3n) \;\; \text{using property (1) and Euclid's Lemma} \\ &\iff 17 \mid 6m + 9n \\ &\iff 17 \mid 6m + 9n - 17n \;\; \text{using property (3)} \\ &\iff 17 \mid 6m - 8n \\ &\iff 17 \mid 2(3m - 4n) \\ &\iff 17 \mid 3m - 4n \;\; \text{using Euclid's Lemma and property (1)} \end{aligned}$$

□

Remark: Notice that each line of reasoning can work in both directions, which is why we could address both implications of the "if and only if" at the same time.

Now let's look at a harder example!

Example 3.5 *Find all positive integers d such that there exists some integer n where*

$$d \mid (n + 3)^2 \text{ and } d \mid (n + 1)(n + 5).$$

Notice that the question asks us to "**find all** positive integers d such that...". Recall that this means we need to:

- Find the set of solutions for d.
- Show that they work.
- Show that no other values for d will work.

We begin by finding some restrictions on the value that d may take.

$$\begin{aligned} d \mid (n+3)^2 &\implies d \mid n^2+6n+9 \\ d \mid (n+1)(n+5) &\implies d \mid n^2+6n+5 \end{aligned}$$

By property (3) we have that:

$$\begin{aligned} d \mid (n+3)^2-(n+1)(n+5) &\implies d \mid (n^2+6n+9)-(n^2+6n+5) \\ &\implies d \mid 4 \end{aligned}$$

This means that any possible value for d must be a divisor of 4. That is, possible values for d are 1, 2 or 4 and **no other values will work**.

To verify that **these solutions are possible**, we can consider $n = 1$ and the two initial conditions are equivalent to $d \mid 16$ and $d \mid 12$, and so $d = 1, 2, 4$ satisfy each of these.

Hence the **all** the solutions for d are 1, 2 and 4. □

4 Division and Divisors

We know that one integer is not always divisible by another integer. However if we adjust the division a little bit and allow a small remainder then the division process always becomes possible. It is known as the **division algorithm** and is formally written as

Theorem 4.1 *For any two given integers n and $d > 0$, there are unique numbers q and r such that $n = dq + r$ and $0 \leq r < d$.*

This theorem mathematically describes the process of division - where if we have a **dividend** (n) and a **divisor** (d), there will always be a *unique* **quotient** (q) and **remainder** (r).

5 Fundamental Theorem of Arithmetic

The most fundamental theorem in number theory on which all the theory rests upon has the very unsurprising name:

Theorem 5.1 (The Fundamental Theorem of Arithmetic) *Every integer $n > 1$ can be uniquely represented as a product of primes. That is, it has a unique representation*

$$n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_k^{a_k}$$

where $p_1, p_2, p_3, \dots p_k$ represent the 1st, 2nd, 3rd prime number and so on, and $a_1, a_2, a_3, \dots, a_k, k$ are non-negative integers. This can be further condensed into the form

$$n = \prod_{i=1}^{k} p_i^{a_i}.$$

This theorem shows that when we **factorise** a number, we **always get the same result**, so it does not matter in which order we find prime factors. For example, if we factorise 30, we can first notice that it is even, i.e. $30 = 2 \cdot 15$, and then get $15 = 3 \cdot 5$. Or we can first notice that 30 is divisible by 5, i.e. $30 = 5 \cdot 6$ and then write $6 = 2 \cdot 3$. In both cases we end up with

$$30 = 2 \cdot 3 \cdot 5.$$

Remark: Although this may seem obvious with the arithmetic that we are used to, there is a field of mathematics called *Algebraic Number Theory* where the Fundamental Theorem of Arithmetic is **not** true. That is, a single number may have **multiple factorisations**.

Let's use this to try solve an example question!

Example 5.2 *What is the least positive integer n such that $60 \times n$ is a cube?*

From the Fundamental Theorem of Arithmetic, we can factorise n into the form

$$n = 2^{a_1}3^{a_2}5^{a_3}7^{a_4}\dots.$$

This means that our desired cube is

$$\begin{aligned}60n &= 2^2 \cdot 3 \cdot 5 \cdot n\\ 60n &= 2^2 \cdot 3 \cdot 5 \cdot 2^{a_1}3^{a_2}5^{a_3}7^{a_4}\dots\\ 60n &= 2^{a_1+2}3^{a_2+1}5^{a_3+1}7^{a_4}\dots\end{aligned}$$

In order to have a cube number, we need to ensure that all its prime factors come in multiples of 3. As we want the minimal value of n, we need the smallest values of $a_1, a_2, a_3, a_4, \dots$ to make the powers of each of the prime factors a multiple of 3.

This means we can choose $a_1 = 1$, $a_2 = a_3 = 2$ and $a_4 = a_5 = \cdots = 0$ so that

$$n = 2 \cdot 3^2 \cdot 5^2 = 450$$

□

Exercise 5.3 *A powerful number is an integer whose prime factors, when squared, remain factors. A perfect power is an integer which can be written as another integer to an integer power. Find the smallest positive integer which is powerful, but not a perfect power.*

Exercise 5.4 *Which numbers have an odd number of factors?*

6 GCD and LCM

The **Greatest Common Divisor** of integers a and b is written as $\gcd(a, b)$, or sometimes just (a, b) for short. If $\gcd(a, b) = 1$, then we call a and b **relatively prime**, or **coprime**. Similarly, we can write the **Lowest Common Multiple** as $\operatorname{lcm}(a, b)$.

At first sight, computation of $\gcd(a, b)$ for given integers a and b looks easy. For example, to compute $\gcd(21, 30)$ we can find the **prime factorisation** of each number:

$$21 = 3 \cdot 7; \quad 30 = 2 \cdot 3 \cdot 5.$$

Then for each prime, we take the largest prime power that divides both numbers. That gives us $\gcd(21, 30) = 3$. However, finding the prime factorisation of numbers can sometimes be **horribly inefficient**, especially when we are dealing with large numbers!

Example 6.1 *Compute* $\gcd(13289, 39673)$.

Factorising 13289 and 39673 without a calculator becomes a challenging task. However there is a way to compute the gcd above quickly! Before we can do that, we need to have a look at some properties of gcd. A useful property of the gcd here is

- For $a, b \in \mathbb{Z}$, $\gcd(a, b) = \gcd(a, b + a) = \gcd(a, b - a)$.

Equipped with this property we can write down our gcd as

$$\begin{aligned}\gcd(13289, 39673) &= \gcd(13289, 39673 - 13289) = \gcd(13289, 26384)\\ &= \gcd(13289, 13095) = \gcd(13289, -194).\end{aligned}$$

We are making numbers smaller! Next, we can make this gcd look a bit nicer with the following properties

- For $a, b \in \mathbb{Z}$, $\gcd(a, b) = \gcd(a, -b)$;
- For $a, b \in \mathbb{Z}$, $\gcd(a, b) = \gcd(b, a)$.

With their help, our gcd becomes $\gcd(194, 13289)$. We are ready to make the numbers even smaller! Before we do that let's consider one more trick which will make things much faster. Let's divide 13289 by 194 with remainder:

$$13289 = 68 \cdot 194 + 97.$$

Then we have

$$\gcd(194, 13289) = \gcd(194, 13289 - 194) = \gcd(194, 13289 - 2 \cdot 194) = \cdots = \gcd(194, 97).$$

The last gcd is easy to compute, it equals 97!

Hence, we compute that $\gcd(13289, 39673) = 97$.

The method we used to attack the problem is called the **Euclidean Algorithm**. That is to find $\gcd(a, b)$, we simply perform multiple divisions where we start with a as our **dividend** and b as our **divisor**. The dividend and divisor of each subsequent division is the divisor and remainder respectively of the previous division. This process is repeated until a remainder of 0 is attained. The GCD is then the **final divisor**.

Another useful application of the Euclidean Algorithm is that it allows us to rewrite the GCD in terms of the original numbers! This is done by starting with the second last line, making the GCD the subject, and working backwards through the Euclidean algorithm.

Example 6.2 *Compute* $\gcd(403, 91)$ *and find integers c and d such that* $\gcd(403, 91) = 403c + 91d$.

To apply the Euclidean Algorithm, we begin by dividing 403 by 91:

$$\begin{aligned}\mathbf{403} &= 4 \cdot \mathbf{91} + \mathbf{39}\\ \mathbf{91} &= 2 \cdot \mathbf{39} + \mathbf{13}\\ \mathbf{39} &= 3 \cdot \mathbf{13}\end{aligned}$$

We now have a remainder of 0 and the final divisor was 13, so we can say that $\gcd(403, 91) = 13$. Next, we write 13 as our subject

$$\begin{aligned}\mathbf{13} &= \mathbf{91} - 2 \cdot \mathbf{39}\\ \mathbf{13} &= \mathbf{91} - 2 \cdot (\mathbf{403} - 4 \cdot \mathbf{91})\\ \mathbf{13} &= 9 \cdot \mathbf{91} - 2 \cdot \mathbf{403}\end{aligned}$$

In fact, rewriting the GCD of two numbers in this form is so useful, we give it a special name:

Theorem 6.3 (Bézout's Identity) *If a and b are integers with greatest common divisor d, then there exist integers x and y such that $d = ax + by$.*

Exercise 6.4 *Find the greatest common divisor of 1643 and 1271 and rewrite the gcd in terms of 1642 and 1271.*

There are indeed many other interesting properties about the gcd and lcm! You may want to play around with a few examples to understand what each of these properties are actually saying.

- For all $a, b \in \mathbb{Z}$, $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$
- For all $a, b, m \in \mathbb{Z}$, $\gcd(ma, mb) = m \gcd(a, b)$
- For all $a, b, m \in \mathbb{Z}$, $\operatorname{lcm}(ma, mb) = m \operatorname{lcm}(a, b)$
- For $a, b, c \in \mathbb{Z}$, if $a \mid bc$ and $\gcd(a, c) = 1$, then $a|b$
- For $a, b, d \in \mathbb{Z}$, if $d \mid a$ and $d \mid b$, then $d| \gcd(a, b)$

These properties can also be proven rigorously!

Example 6.5 *Prove that for all $a, b \in \mathbb{Z}$, $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$.*

To prove statements like this, it is convenient to let $d = \gcd(a, b)$. This means that we can rewrite a and b as

$$a = kd \quad \text{and} \quad b = ld \quad \text{such that} \quad \gcd(k, l) = 1$$

Hence, $\operatorname{lcm}(a, b) = kld$ so we have that

$$ab = kld^2$$

and

$$\gcd(a, b) \cdot \operatorname{lcm}(a, b) = d \cdot kld = kld^2.$$

Hence, we see that $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$. □

Exercise 6.6 *Prove the remaining properties.*

7 Additional Problems

1. Prove that every prime number greater than 3 leaves a remainder of either 1 or 5 when divided by 6.
2. If $935712 \times N$ is a perfect cube for some positive integer N, find the minimum possible value for N.
3. Let p, q, r be prime numbers such that $pqr(p + q + r)$ is a perfect square. Find all possible values of (p, q, r).
4. (a) What is the maximum number of terms in an arithmetic sequence of primes with common difference 6?

   (b) What is the minimum common difference for an increasing arithmetic sequence of 6 primes.