MATH1081 – Discrete Mathematics

Topic 2 – Number theory and relations
Lecture 2.01 – Divisibility and greatest common divisors

Lecturer: Dr Sean Gardiner – sean.gardiner@unsw.edu.au

Introduction to number theory and relations

Number theory is primarily concerned with the study of integers and subsets of the integers. So for this topic we will mostly be working with:

- The integers $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$.
- The positive integers $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$.
- The natural numbers $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.

For these and all other number sets we have encountered ($\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$), if we add or multiply any two elements from one of the sets, we attain another element from that set. But for the operation of division, the integers and its subsets are distinguished by the fact that this property does not hold – dividing one integer by another non-zero integer does not guarantee an integer result.

Number theory is one of the most fundamental branches of Mathematics, and is still relevant in the modern era especially considering its applications to cryptography.

Towards the end of this topic, we will also address the topic of mathematical relations, which is a natural generalisation of what we have already learned about functions, and provides more structure to our understanding of divisibility and modular arithmetic.

Divisibility

Definition. Given two integers a and b, we say a divides b if we can write $b = ak$ for some integer k. We might also say:

- a is a divisor of b,
- a is a factor of b,
- b is divisible by a, or
- b is a multiple of a.

Notation. The expression $a \mid b$ is read as "a divides b" and is equivalent to writing $b = ak$ for some integer k. The expression $a \nmid b$ is read as "a does not divide b", and means that $b \neq ak$ for any integer k.

Example. Decide whether the following statements are true or false.

- $3 \mid 15$ is true since $15 = 3 \times 5$ and $5 \in \mathbb{Z}$.
- $15 \mid 3$ is false since $3 = 15 \times \frac{1}{5}$ but $\frac{1}{5} \notin \mathbb{Z}$.
- $3 \mid 3$ is true since $3 = 3 \times 1$ and $1 \in \mathbb{Z}$.
- $-5 \mid 15$ is true since $15 = (-5) \times (-3)$ and $-3 \in \mathbb{Z}$.
- $0 \mid 3$ is false since there is no integer k such that $3 = 0 \times k$.
- $3 \mid 0$ is true since $0 = 3 \times 0$ and $0 \in \mathbb{Z}$.
- $0 \mid 0$ is true since $0 = 0 \times 1$ (for example) and $1 \in \mathbb{Z}$.

Divisibility properties

The divisibility relation has many useful properties. Some of the most important are the following.

Lemma. For all integers a, we have $a \mid a$.

Proof. Since $a = a \times 1$ and $1 \in \mathbb{Z}$, we have by definition that $a \mid a$.

Lemma. For all integers a, b, c, if $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof. Since $a \mid b$, we have $b = ak$ for some $k \in \mathbb{Z}$, and since $b \mid c$, we have $c = bl$ for some $l \in \mathbb{Z}$. So $c = (ak)l = a(kl)$ where $kl \in \mathbb{Z}$, so $a \mid c$.

Lemma. For all integers a, b, c, if $a \mid b$ and $a \mid c$, then $a \mid bx + cy$ for any $x, y \in \mathbb{Z}$.

Proof. Since $a \mid b$, we have $b = ak$ for some $k \in \mathbb{Z}$, and since $a \mid c$, we have $c = al$ for some $l \in \mathbb{Z}$. So $bx + cy = (ak)x + (al)y = a(kx + ly)$ where $kx + ly \in \mathbb{Z}$, so $a \mid bx + cy$.

We can deduce other useful facts from the above properties. For example, setting $c = 0$ in the third lemma shows that if $a \mid b$ then $a \mid bm$ for any integer m. Combining this with the first lemma shows that $a \mid am$ for any integer m.

Prime numbers

Definition. A prime number (or just a prime) is any $p \in \mathbb{N}$ such that $p > 1$ and the only positive divisors of p are 1 and p.

The first few prime numbers are $2, 3, 5, 7, 11, 13, 17, 19, \ldots$.

Definition. A composite number is any natural number that is not 0, 1, or a prime number.

The first few composite numbers are $4, 6, 8, 9, 10, 12, \ldots$.

Theorem. There are infinitely many prime numbers.

Proof. See Angell: Slide 3.53 (or Gardiner: Lecture 3.07, Example 5).

To determine if a natural number n is prime, a standard approach is to check whether it is divisible by all known primes less than or equal to $\sqrt{n}$. (See Problem Set 3, Question 25.)

For example, 1009 is prime because it is not divisible by any of the primes less than or equal to $\lfloor \sqrt{1009} \rfloor = 31$.

Fundamental Theorem of Arithmetic

Theorem. (Fundamental Theorem of Arithmetic)
Every natural number greater than 1 has a unique prime factorisation. That is, given any positive integer $n > 1$, it can be written uniquely in the form

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k},$$

where each $p_1, p_2, \ldots, p_k$ is a prime number, $p_1 < p_2 < p_3 < \cdots < p_k$, and $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{Z}^+$ for some $k \in \mathbb{Z}^+$.

Proof. See Angell: Slide 3.76 (or Gardiner: Lecture 3.08, Example 4).

For example, the prime factorisation of 12 is $2^2 \times 3$.

Example. Find the prime factorisations for each of the integers from 21 to 25.

- $21 = 3 \times 7$.
- $22 = 2 \times 11$.
- $23 = 23$.
- $24 = 2^3 \times 3$.
- $25 = 5^2$.

Common divisors

Definition. A common divisor of two integers a and b is any integer d such that both $d \mid a$ and $d \mid b$.

Example. Which of the following are common divisors of 12 and 18?

- 1 is a common divisor of 12 and 18 because $1 \mid 12$ and $1 \mid 18$.
- -6 is a common divisor of 12 and 18 because $-6 \mid 12$ and $-6 \mid 18$.
- 9 is not a common divisor of 12 and 18 because $9 \mid 18$ but $9 \nmid 12$.

Definition. Two integers a and b are coprime or relatively prime if and only if their only common divisors are 1 and -1. Equivalently, two integers are coprime if and only if their only positive common divisor is 1.

Example. Which of the following pairs of numbers are coprime?

- 2 and 3 are coprime because 1 is their only positive common divisor.
- 9 and -10 are coprime because 1 is their only positive common divisor.
- 12 and 18 are not coprime because they have positive common divisors other than 1, for example 2, 3, or 6.
- 0 and 1 are coprime because 1 is their only positive common divisor.

Greatest common divisors

Definition. The greatest common divisor (GCD) of two integers a and b (when a and b are not both 0), denoted $\gcd(a, b)$, is the natural number $d \in \mathbb{N}$ such that

- both $d \mid a$ and $d \mid b$, and
- for all $c \in \mathbb{N}$, if $c \mid a$ and $c \mid b$, then $c \leq d$.

For example, $\gcd(3, 5) = 1$ and $\gcd(12, 18) = 6$.

If the prime factorisations of a and b are known, then $\gcd(a, b)$ can easily be found by taking the product of the lower powers of each prime factor. For example, $\gcd(108, 72) = \gcd(2^2 \times 3^3, 2^3 \times 3^2) = 2^2 \times 3^2 = 36$.

Example. Find $\gcd(2^3 \times 3^2 \times 7, 2^2 \times 3 \times 5)$.

Solution. We have $\gcd(2^3 \times 3^2 \times 7, 2^2 \times 3 \times 5) = 2^2 \times 3^1 \times 5^0 \times 7^0 = 12$.

Alternate definition. The greatest common divisor $\gcd(a, b)$ of two integers a and b is the natural number $d \in \mathbb{N}$ such that

- both $d \mid a$ and $d \mid b$, and
- for all $c \in \mathbb{N}$, if $c \mid a$ and $c \mid b$, then $c \mid d$.

With this definition, the value of $\gcd(0, 0)$ is well-defined and equals 0.

Properties of the GCD

Some useful properties of the GCD are given below. Suppose a, b, c, q are integers.

- **Property 1.** $\gcd(a, 1) = 1$.
- **Property 2.** $\gcd(a, 0) = |a|$.
- **Property 3.** $\gcd(a, \gcd(b, c)) = \gcd(\gcd(a, b), c)$.
- **Property 4.** $\gcd(ac, bc) = |c| \gcd(a, b)$.
- **Property 5.** If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.
- **Property 6.** If $a = qb + c$, then $\gcd(a, b) = \gcd(b, c)$.

  Proof. Since $a = qb + c$ and $\gcd(b, c)$ is a common divisor of b and c, it must also be a divisor of a (by the third lemma on slide 3). So $\gcd(b, c) \leq \gcd(a, b)$, since $\gcd(a, b)$ is the greatest common divisor of a and b.

  Similarly, since $c = a - qb$ and $\gcd(a, b)$ is a common divisor of a and b, it must also be a divisor of c. So $\gcd(a, b) \leq \gcd(b, c)$, since $\gcd(b, c)$ is the greatest common divisor of b and c.

  Combining both these inequations, we deduce that $\gcd(a, b) = \gcd(b, c)$.

Least common multiples

Definition. The least common multiple (LCM) of two non-zero integers a and b, denoted $\mathrm{lcm}(a, b)$, is the positive integer $d \in \mathbb{Z}^+$ such that

- both $a \mid d$ and $b \mid d$, and
- for all $c \in \mathbb{Z}^+$, if $a \mid c$ and $b \mid c$, then $d \leq c$.

For example, $\mathrm{lcm}(3, 5) = 15$, and $\mathrm{lcm}(4, 6) = 12$.

If the prime factorisations of a and b are known, then $\mathrm{lcm}(a, b)$ can easily be found by taking the product of the higher powers of each prime factor. For example, $\mathrm{lcm}(108, 72) = \mathrm{lcm}(2^2 \times 3^3, 2^3 \times 3^2) = 2^3 \times 3^3 = 216$.

Example. Find $\mathrm{lcm}(2^3 \times 3^2 \times 7, 2^2 \times 3 \times 5)$.

Solution. We have $\mathrm{lcm}(2^3 \times 3^2 \times 7, 2^2 \times 3 \times 5) = 2^3 \times 3^2 \times 5^1 \times 7^1 = 2520$.

Fact. For any positive integers a and b, we have $\gcd(a, b)\,\mathrm{lcm}(a, b) = ab$.

Alternate definition. The least common multiple $\mathrm{lcm}(a, b)$ of two integers a and b is the natural number $d \in \mathbb{N}$ such that

- both $a \mid d$ and $b \mid d$, and
- for all $c \in \mathbb{N}$, if $a \mid c$ and $b \mid c$, then $d \mid c$.

With this definition, $\mathrm{lcm}(a, b)$ is well-defined even when a or b is 0.

Case study: Natural numbers as sets

(Remember that “case studies” are additional content and not examinable.)

In the early 1920s, Ernst Zermelo and Abraham Fraenkel set out to describe set theory entirely axiomatically, meaning they wanted to rigorously define/prove all aspects of set theory using only a minimal list of assumed axioms (fundamental truths). Their motivation was to build up a system that avoided the construction paradoxes like Russell’s paradox. The resulting so-called Zermelo-Fraenkel set theory is still used as the standard model for axiomatic set theory today.

Soon thereafter, at the age of 19, mathematician and computer scientist John von Neumann described a way of defining the natural numbers in the context of ZF set theory. The system defines the number 0 as being represented by the empty set, and for each positive integer n, the number $n+1$ is defined by $n+1 := n \cup \{n\}$. This construction allows the number n to be represented by the set with cardinality n.

$$\begin{array}{lllll}
0 & := & \{\} & = & \{\} \\
1 & := & \{0\} & = & \{\{\}\} \\
2 & := & \{0,1\} & = & \{\{\},\{\{\}\}\} \\
3 & := & \{0,1,2\} & = & \{\{\},\{\{\}\},\{\{\},\{\{\}\}\}\}.
\end{array}$$