MATH 1200 Section A (Tutorial 02)
Tutorial 11: The Integers, Cardinality of Sets

---

1. The Integers

Definition 1. Let $a, b \in \mathbb{Z} \setminus \{0\}$ be nonzero integers. The largest d such that $d \mid a$ and $d \mid b$ is called the *greatest common divisor of a and b*. The greatest common divisor is dentoed by $\gcd(a, b) = \max\{d \in \mathbb{N} : d \mid a \text{ and } d \mid b\}$.

Example 1. What is the greatest common divisor of the following numbers:

(a) 24 and 36

24: 1, 2, 3, 4, 6, 8, 12, 24
36: 1, 2, 3, 4, 6, 9, 12, 18, 36.
gcd(24, 36) = 12

(b) 17 and 22

17: 1, 17
22: 1, 2, 11, 22
gcd(17, 22) = 1

Definition 2. Two integers $a, b \in \mathbb{Z} \setminus \{0\}$ is said to be *relatively prime* if $\gcd(a, b) = 1$. The integers $a_1, a_2, ..., a_n \in \mathbb{Z} \setminus \{0\}$ are said to be *pairwise relatively prime* if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

Example 2. From Example 1(b), 17 and 22 are relatively prime.

Example 3. Determine whether the following integers are pairwise relatively prime.

(a) 10, 17, 21

gcd(10, 17) = 1
gcd(10, 21) = 1
gcd(17, 21) = 1
10, 17, 21 relatively prime.

(b) 10, 19, 24

gcd(10, 19) = 1
gcd(19, 24) = 1
gcd(10, 24) = 2 ≠ 1
10, 19, 24 <u>not</u> relatively prime.

In order to find the greatest common divisor between two large numbers, we provide a more efficient method of finding the greatest common divisor, which is called the *Euclidean algorithm*, which has been known since ancient times and has been named after the Greek mathematician Euclid, who included a description of this algorithm in his book called *The Elements*.

Recall: Division Algorithm $a = nq + r$.

Example 4. Find the greatest common divisor of 414 and 662 using the Euclidean algorithm.

$662 = 414 \cdot 1 + 248$
$441 = 248 \cdot 1 + 166$
$248 = 166 \cdot 1 + 82$
$166 = 82 \cdot 2 + 2$
$82 = 2 \cdot 41$

Hence, $\gcd(414, 662) = 2$.

Remark: The $\gcd(414, 662) = 2$ because the last non zero remainder is 2.

An important result we will use is that the greatest common divisor of two integers a and b can be expressed in the form $xa + yb$ where $x, y \in \mathbb{Z}$. That is, the greatest common divisor of a and b can be expressed as a linear combination.

Theorem 1 (Bèzout's Theorem). *If $a, b \in \mathbb{N}$, then there exists $x, y \in \mathbb{Z}$ such that* $\gcd(a, b) = xa + yb$.

Example 5. Use Bèzout's Theorem to show that $\gcd(252, 198) = 18$ as a linear combination of 252 and 198 by working backwards through the steps of the Euclidean algorithm.

Forward using Euclidean Algorithm:

$252 = 198 \cdot 1 + 54 \implies 54 = 252 - 1 \cdot 198$
$198 = 54 \cdot 3 + 36 \implies 36 = 198 - 3 \cdot 54$
$54 = 36 \cdot 1 + 18 \implies 18 = 54 - 1 \cdot 36.$
$36 = 18 \cdot 2$

Backward using Euclidean Algorithm:

① $18 = 54 - 1 \cdot 36$
② $36 = 198 - 3 \cdot 54$
② $\Rightarrow$ ① $18 = 54 - 1(198 - 3(54))$
$= 54 - 1(198) + 3(54)$
$= 4(54) - 1(198)$ ③

$54 = 252 - 1 \cdot 198$ ④
④ $\Rightarrow$ ③ $18 = 4(252 - 1(198)) - 1(198)$
$= 4(252) - 4(198) - 1(198)$
$= 4(252) - 5(198)$

Bèzout's Theorem,
$18 = 4 \cdot 252 - 5 \cdot 198.$

Definition 3. An integer $p > 1$ is called *prime* if the only positive factors of p are 1 and p. A positive integer that is greater than 1 is not prime and is called composite.

The primes are the building blocks of positive integers, as the fundamental theorem of arithmetic shows.

Theorem 2 (Fundamental Theorem of Arithmetic). *Every integer greater than 1 can be written uniquely as a prime or as a product of two or more primes, where the prime factors are written in order of nondecreasing size.*

Example 6. The prime factorizations of 100, 641, 999, and 1024 are given by

$$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$$

$$641 = 641 \text{ (prime)}$$

$$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$$

$$1024 = 2^{10}$$

2. Cardinality of Sets

Recall we have defined the cardinality of sets in a previous tutorial:

Definition 4. Let A be a set.

- The *cardinality of a set A* is the number of elements in the set and we denote it by $|A|$.
- The set A is said to be an *infinite set* if there are infinitely many elements in A.

Example 7. $A = \{1, 2, 3\}$ has 3 elements, while $B = [0, 1]$ has infinitely many elements.

Definition 5. A set that is either finite or has the same cardinality as the set of positive integers is said to be *countable*. A set that is not countable is called *uncountable.* When an infinite set S is countable, we denote the cardinality of S by $\aleph_0$ (where $\aleph$ is aleph, the first letter of the Hebrew alphabet). We write $|S| = \aleph_0$ and say that S has cardinality "aleph null".

Proposition 1. *The set of all integers is countable.*

Proof. We can list all integers in a sequence by starting at 0 and alternating between positive and negative integers: $0, 1, -1, 2, -2, \ldots$. □

Alternatively, we can find a bijection between $\mathbb{N}$ and $\mathbb{Z}$

Define the function:

$$f(x) = \begin{cases} \frac{x}{2} & \text{if } x \text{ is even} \\ \frac{1-x}{2} & \text{if } x \text{ is odd.} \end{cases}$$

Then $f(x)$ is such a bijection. (Exercise)

Consequently $\mathbb{Z}$ is countable.

Proposition 2. *The set of all positive rational numbers are countable.*

Proof. ☐

$$\begin{array}{cccccc} \frac{1}{1} & \frac{2}{1} & \frac{3}{1} & \frac{4}{1} & \frac{5}{1} & \cdots \\ \frac{1}{2} & \frac{2}{2} & \frac{3}{2} & \frac{4}{2} & \frac{5}{2} & \cdots \\ \frac{1}{3} & \frac{2}{3} & \frac{3}{3} & \frac{4}{3} & \frac{5}{3} & \cdots \\ \frac{1}{4} & \frac{2}{4} & \frac{3}{4} & \frac{4}{4} & \frac{5}{4} & \cdots \\ \frac{1}{5} & \frac{2}{5} & \frac{3}{5} & \frac{4}{5} & \frac{5}{5} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \end{array}$$

Because all positive rational numbers are listed once, the set of positive rational numbers is countable.

The above argument is called the *Cantor's Diagonalization Argument*, which is used to prove that the set of real numbers is uncountable.

Proposition 3. *The set of all real numbers is uncountable.*

Proof. ☐

To show that the set of real numbers is uncountable, we suppose that the set of real numbers is countable and arrive at a contradiction. Then the subset of the real numbers that fall between 0 and 1 would also be countable.

Under this assumption, the real numbers between 0 and 1 can be listed in some order, say $r_1, r_2, r_3, \ldots$, Let the decimal representation of the real numbers be

$r_1 = 0.d_{11}d_{12}d_{13}d_{14}\cdots$

$r_2 = 0.d_{21}d_{22}d_{23}d_{24}\cdots$

$r_3 = 0.d_{31}d_{32}d_{33}d_{34}\cdots$

$\vdots$

where $d_{ij} \in \{0, 1, 2, 3, \ldots, 9\}$.

Then form a new real number with the decimal expansion $r = 0.d_1d_2d_3d_4\cdots$ where the decimal digits are determined by the following rule:

$$d_i = \begin{cases} 4 & \text{if } d_{ii} \neq 4 \\ 5 & \text{if } d_{ii} = 4 \end{cases}$$

Then every real number has a unique decimal expansion.

Therefore, the real number r is not equal to any of $r_1, r_2, \ldots$ because the decimal expansion of r differs from the decimal expansion of r_i in the ith place to the right of the decimal point for each i.

Because there is a real number r between 0 and 1 that is not on the list, the assumption that all real numbers between 0 and 1 could be listed, must be false.

Therefore, all real numbers between 0 and 1 cannot be listed, so the set of real numbers between 0 and 1 is uncountable.

Any set with an uncountable subset is also uncountable.
Therefore, the set of real numbers is uncountable.