

**Comments on subtle points of
Sections 1.1 and 1.2**

1. The well ordering principal and related ideas.

The *well ordering principal* of \mathbb{N} , the non-negative integers, states that any non-empty set of \mathbb{N} has a least element. (From a utilitarian standpoint, this means that if $S \subseteq \mathbb{N}$, $S \neq \emptyset$, then there is an $n \in S$, such that $n \leq m$ for all other $m \in S$.)

This is an **axiom** - you don't/can't prove it. It is a "self evident" property of \mathbb{N} . However, one can show that it is logically equivalent to mathematical induction, or the fact that every integer has a successor.

More generally, if $S \subseteq \mathbb{Z}$ is a non-empty subset of integers (not-necessarily non-negative) that is bounded below, that is there is a $p \in \mathbb{Z}$ such that $p \leq s$ for all $s \in S$, then S has a least element. NOTE: this means that there is an element $m \in S$ (actually in the set) such that $m \leq s$ for all $s \in S$.

Contrast this with the real numbers: 0 is less than every element of $S = (0, \infty) \subseteq \mathbb{R}$, but 0 is not actually in S , it is the infimum.

Alternatively, if S is a non-empty **finite** set of real numbers, or integers, then S contains BOTH a maximum element and minimal element.

2. Divisors.

In \mathbb{Z} we use "divides" as a very specific term:

When we say a **divides** b , in \mathbb{Z} , which we denote by $a|b$, we should realize that this is *terminology*. The functional usage is a *divides* b **MEANS** that b is a multiple of a .

So if we are given $a, b \in \mathbb{Z}$, $a|b$, then we should immediately realize that the utilitarian view is b is a multiple of a so there exists $r \in \mathbb{Z}$ such that $b = ar$.

3. The division algorithm.

The division algorithm states:

Result 1 If $a, b \in \mathbb{Z}$, $b > 0$, then there exist unique integers $q, r \in \mathbb{Z}$, $0 \leq r < b$, such that $a = bq + r$.

There are two steps to the proof of this:

- **EXISTENCE:** We prove that there are such q and r by examining the set $S = \{a - bq : q \in \mathbb{Z}\}$. We must argue that S has non-negative numbers. Once we establish that we let r be the least non-negative number in the set - actually in the non-empty set $S \cap \mathbb{N}$, and let q be the value such that $a = bq + r$.
- **UNIQUENESS:** We show that r and q are unique by *assuming that they are not*, that is, suppose there exist $p, s \in \mathbb{Z}$ such that $0 \leq s < b$, and $b = ap + s$. Now show that b divides $|r - s|$ (absolute value), and $0 \leq |r - s| < b$. This implies $r = s$ (WHY?), and thus $r = s$, $p = q$.

4. Ideals in \mathbb{Z} :

We have a result that says

Result 2 If $I \subseteq \mathbb{Z}$ is closed under addition and subtraction, then $I = \{0\}$, or $I = b\mathbb{Z} = \{bz : z \in \mathbb{Z}\}$, where b is the smallest positive element of S .

This is a typical **OR** problem.

Notice, either $I = \{0\}$ or it doesn't.

If $I = \{0\}$, then the result is true.

Otherwise, $I \neq \{0\}$, and there is $a \in I$, $a \neq 0$.

Now: prove I has at least one positive element (HOW?); let b be the smallest positive element of I .

Then, for any $s \in I$, $s = bq + r$, $0 \leq r < b$. This in turn implies $s - bq = r \in I$, since I is closed under subtraction, so $r \in I$. This then implies $r = 0$, so $s = bq$ (WHY?), and thus $I \subseteq b\mathbb{Z}$.

We complete the proof by showing that $b\mathbb{Z} \subseteq I$.

Comments:

- (a) This is standard for proving two sets are equal. To prove that the sets A and B are equal we show that $A \subseteq B$ and $B \subseteq A$.
- (b) Note that this result also implies the following: if $c \in I = b\mathbb{Z}$, and $t \in \mathbb{Z}$, then $ct \in I = b\mathbb{Z}$. Prove this.

5. Greatest Common Divisors.

For two integers a and b , not both 0 (usually BOTH non-zero) we have been introduced to two different definitions of the greatest common divisor of a and b .

For $a, b \in \mathbb{Z}$, d is a common divisor of a and b if it divides both (both a and b are multiples of d).

Commonly, we are taught that the **greatest common divisor** of a and b is the common divisor of the two that is *numerically* the largest. [Note that this is why we say *both non-zero* - if $a = b = 0$, then a and b are both multiples of all integers.]

We can establish that the (numerically) largest common divisor of a and b exists quite easily.

Let S be the set of all positive common divisors of a and b . S is a finite non-empty set. It's non-empty since $1 \in S$, and finite since all common divisors of a and b must be less than or equal to $\max\{|a|, |b|\}$. [This again requires that one of the numbers be non=zero.]

Since S is finite it has a maximum element - that is, there is a (numerically) greatest common divisor of a and b

However, this is not the definition that we use. The gcd is defined as follows.

For $a, b \in \mathbb{Z}$, $a \neq 0$ or $b \neq 0$, the **greatest common divisor** of a and b is the integer $d \geq 1$, such that

- d is a common divisor of a and b ,
- if d_1 is any other common divisor of a and b , then $d_1 | d$.

In class, we discussed the fact that these two notions are equivalent. Can you prove it? Can you see that our definition is more useful?