1) Division Algorithm

Well Ordering Axiom
every nonempty subset of the set of non-negative integers contains a smallest element
Theorem: Division Algorithm
Let a,b be integers with $b > 0$.
Then $\exists q$ and $\exists r \in \mathbf{Z}$ (both q and r are unique) such that

$$a = bq + r$$

(2) Divisibility

Definition
Let a and b be integers with $b \neq 0$ then $b|a$ if and only if a = bc for $c \in \mathbb{Z}^+$
In symbols:

- $b|a$ writes out "b divides a"
- $b \times a$ writes out "b does not divides a"

Remarks

- every divisor of the nonzero integer a is less than or equal to $|a|$
- a nonzero integer has only finitely many divisors

Greatest Common Divisors (GCD)
Let a and b be both integers, both not 0. The gcd of a and b is the largest integer d that divides both a and b.

- $d|a$ and $d|b$
- if $c|a$ and $c|b$ then $c \leq d$
- usually denoted as (a,b)

Theorem 1.2
Let a and b be integers not 0 and let d be the GCD. Then there exists a u and v (not necessarily unique) such that

$$d = (au + bv)$$

Warning Does not imply that (a,b) = d (check exercise 25)
Corollary 1.3
Let a and b be integers, both not 0, then d is a GCD of a and b if and only if

- $d|a$ and $d|b$
- if $c|a$ and $c|b$ then $c|d$

Theorem 1.4
If $a|bc$ and $(a,b) = 1$ then $a|c$

(3) Primes and Unique Factors

Prime
an integer is prime if the only divisors are ± 1 and $\pm$ itself

- p is prime if and only if - p is prime
- if p and q are prime and $p|q$, then $p = \pm q$

Theorem 1.5
Let p be an integer with $p \neq 0, \pm 1$ then p is prime if and only if whenever $p|bc$ then $p|b$ or $p|c$
Corollary 1.6
If p is prime and $p|a_1 a_2 a_3 ... a_n$ then p divides at least one of the
Theorem 1.7
Every integer n except 0, ± 1 is a product of primes.
Theorem 1.8 Fundamental Theorem of Arithmetic
Every integer n except 0 and ± 1 is a product of primes.
Prime factorization is unique in the following: if

$$n = p_1 p_2 p_3 ... p_r$$

and

$$n = q_1 q_2 ... q_s$$

with p_i, q_j prime then r = s and after reordering

$$p_1 = \pm q_1 \; ... p_r = \pm q_r$$

Corollary 1.9
Every integer $n > 1$ can be written in one and only one way in the form

$$n = p_1 p_2, ..., p_r$$

where the p are positive primes such that

$$p_1 < p_2 < ... < p_r$$

Theorem 1.10
Let n $>$ 1 if n has no positive prime factors less than or equal to $\sqrt{n}$ then n is prime.