1 Basics

$\mathbb{N}$ denotes the set of natural numbers 0,1,2,3,..., and let $\mathbb{Z}$ and $\mathbb{Q}$ denote the sets of integers and rational numbers.

We accept as known the fact that these sets are linearly ordered: *ie.* there is a relation $\leq$ with the usual properties. (See Rosen 6.6 for the notions of linear ordering) Also the operations of addition and multiplication are compatible with $\leq$ in familiar ways. For example, if $a > b$ and $c > 0$, then $a + c > b$ and $ac > bc$.

A frequently used result will be the

**Archimedean Property 1.1.** If $r$ and $s$ are two positive rational numbers, then there exists a positive integer $n$ such that $nr > s$.

*Proof.* Supply a proof. □

An axiom that we accept for $\mathbb{N}$ is

**Well-Ordering Principle (WOP) 1.2.** Any non-empty subset of $\mathbb{N}$ contains a least element.

This is closely related to two other axioms:

**Principle of Mathematical Induction (PMI) 1.3.** Suppose $A$ is a subset of $\mathbb{N}$ possessing the following two properties:

1. $0 \in A$.
2. If $k \in A$ then $k + 1 \in A$.

Then $A = \mathbb{N}$.

**Second Principle of Mathematical Induction 1.4.** Let $A$ be a subset of $\mathbb{N}$ possessing the following two properties:

1. $0 \in A$.
2. If $\{0, 1, \ldots, k\} \subseteq A$, then $k + 1 \in A$. 

1
Then $A = \mathbb{N}$.

**Proposition 1.5.** The above three axioms are equivalent.

**Proof.**

**WOP implies Second PMI:** you supply the proof.

**Second PMI implies PMI:** you supply the proof.

**PMI implies WOP:** We assume PMI is true. Instead of directly proving WOP let us first consider the following statement (call it $P(k)$.)

Any non-empty subset of $\{0, 1, \ldots, k\}$ has a least element.

We will establish that $P(k)$ is true for every integer $k \geq 0$, using PMI. Indeed, if $k = 0$, any non-empty subset of $\{0\}$ must be $\{0\}$ itself and $0$ is its least element. So $P(0)$ is true.

Assume now that $P(k)$ is true. As usual we will show that $P(k + 1)$ is true. Let $C$ be a non-empty subset of $\{0, 1, \ldots, k, k + 1\}$. If $C$ does not contain $k + 1$, then since it is a non-empty subset of $\{0, 1, \ldots, k\}$, it has a least element by $P(k)$. On the other hand, if $k + 1 \in C$ and $C$ has other elements, then $C - \{k + 1\}$ is a non-empty subset of $\{0, 1, \ldots, k\}$, and hence $C - \{k + 1\}$ contains a least element which is also the least element of $C$. Lastly, if $k + 1 \in C$ and $C$ has no other elements, then $k + 1$ is the least element of $C$. Thus in each of the three cases, we have shown that $C$ contains a least element, hence $P(k + 1)$ is true. Hence by PMI, $P(k)$ is true for every integer $k \geq 0$.

Now back to our task. Suppose $B$ is a non-empty subset of $\mathbb{N}$. Hence it contains a number $k$. Consider the subset $B'$ of $B$ consisting of all numbers in $B$ which are $\leq k$. By $P(k)$ which we just proved, $B'$ contains a least element $l$. Clearly $l$ is also a least element in $B$. □

**The Division Algorithm 1.6.** Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist integers $q, r$ where $0 \leq r < b$ and $a = qb + r$. Furthermore, $q, r$ are unique for given $a$ and $b$.

**Proof.** I will sketch a proof and let you write it up: First case: $a \geq 0$. Then let $n$ be the least natural number such that $qb \geq a$. (why does $n$ exist?). Choose $q$ to be $n - 1$ and establish that if $r = a - qb$ then $0 \leq r < b$.

Second case: if $a < 0$ the first case leads you to an answer in the second case by considering $a' = -a$ which is in the first case. Uniqueness: Suppose $q', r'$ are other possible solutions. Suppose $q > q'$. Then $q \geq q' + 1$, hence $r = a - qb \leq a - (q' + 1)b = r' - b < 0$, a contradiction! Likewise, $q' > q$ leads to a contradiction. Etc, etc, etc. □
Definition 1.7. If $a, b \in \mathbb{Z}$, we say that ‘$a$ divides $b$’ if $\exists k \in \mathbb{Z}$ such that $ak = b$, and we denote is as $a|b$.

Lemma 1.8. If $n|a$ and $n|b$ then $n|(ra + sb)$ where all letters denote integers.

Proof. Supply the proof. \hfill \Box

Definition 1.9. If $a, b \in \mathbb{Z}$, not both zero, then the greatest common divisor of $a$ and $b$ is a positive integer $d$ (denoted $(a, b)$) satisfying

- $d|a$ and $d|b$.
- If $c \in \mathbb{Z}$ and $c|a$ and $c|b$, then $c|d$.

Proposition 1.10. Let $a, b \in \mathbb{Z}$, not both zero. Then $(a, b)$ exists and is unique, and can be found specifically as the smallest positive integer linear combination of $a$ and $b$.

Proof. Let $I = \{xa + yb|x, y \in \mathbb{Z}\}$. By choosing $x$ and $y$ of the same sign as $a$ and $b$, we see that $I$ contains positive integers. By WOP, $I$ hence contains a smallest positive integer $d$. We must show that $d$ satisfies the two conditions of 1.9. Since $d$ is itself of the form $xa + yb$, the second condition is clear from lemma 1.8. Hence we need just show that $d|a$ and leave you to likewise show $d|b$.

Now by the Division Algorithm, $\exists q, r$ such that $a = qd + r$, with $0 \leq r < d$. Now $d = xa + yb$ (for some $x, y$) so $r = (1 - qx)a + (-qy)b$ which squarely puts it in $I$. Since $r < d$ and $d$ was the smallest positive element of $I$, $r$ can only be 0. Thus $a = qd$ or $d|a$.

For the uniqueness of $d$, if a positive number $d'$ exists with the same two properties as $d$, I will let you verify that $d|d'$, hence $d \leq d'$ as both are positive etc, etc, etc. \hfill \Box

Lemma 1.11. $a$ and $b$ are called relatively prime if $(a, b) = 1$. Then $a$ and $b$ are relatively prime iff $\exists x, y \in \mathbb{Z}$ such that $ax + by = 1$.

Proof. Fill in the necessary two or three lines. \hfill \Box

Lemma 1.12. Suppose $a, b$ are relatively prime. Then $a^n, b^m$ are relatively prime for any positive exponents $n, m$.

Proof. Hint: take the $(n + m)$-th power of the linear combination in 1.11. Try some easy examples first like $n = 2, m = 3$ and review the binomial theorem. \hfill \Box
Lemma 1.13. Suppose $p$ is an integer relatively prime to both $a$ and $b$. Then $p$ is relatively prime to $ab$. Conversely, if $p$ is relatively prime to $ab$, then $p$ is relatively prime to both $a$ and $b$. More generally, the same holds if we replace a product of two integers $a, b$ with the product of any number of integers.

Proof. Supply the proof.

Lemma 1.14. Suppose $a_1, a_2$ are relatively prime and each divides $b$. Then $a_1a_2$ divides $b$

Proof. Supply the proof.

Proposition 1.15. Suppose that $(p, a) = 1$ and $p|(ab)$. Prove that $p|b$.

Proof. Supply proof.

Proposition 1.16. Suppose $(n, m) = 1$. Then $(a, nm) = (a, n)(a, m)$. In particular, any divisor $d$ of $nm$ can be uniquely factored as $d = d_1d_2$, where $d_1|n, d_2|m$.

Proof. Supply proof.

Definition 1.17. Let $a, b$ be two integers, neither zero. The least common multiple of $a$ and $b$ (lcm($a, b$)) is a positive integer $l$ satisfying the following

- $a|l, b|l$.
- If $a|l', b|l'$, then $l|l'$

Proposition 1.18. The lcm of $a$ and $b$ exists, is unique and is given by $|ab|/(a, b)$.

Proof. It is evident from the definitions that the gcd and lcm of $a, b$ are the same as the gcd and lcm of $\pm a, \pm b$ (if the lcm does exist!). So we will assume that $a$ and $b$ are both positive to avoid the absolute value signs.

Now positive common multiples of $a$ and $b$ certainly exist (eg. $ab$ is one), hence by WOP there is a smallest common multiple, call it $l$. We claim that $l$ satisfies both of the conditions of the definition. The first condition needs no discussion. Now suppose $l'$ is such that $a|l', b|l'$. Using the Division Algorithm, let

$$l' = ql + r, 0 \leq r < l.$$
Then $a|r$ since it divides both $l'$ and $l$, likewise $b|r$. Our choice of $l$ was such that $r$ being smaller, must be 0. Hence $l|l'$.

For uniqueness, let $l'$ be another number satisfying the definition of the lcm of $a$ and $b$, in addition to the $l$ we just found. The both $l$ and $l'$ are divisible by $a$ and $b$. Using the second part of the definition, $l|l'$ and $l'|l$. Since both are positive, $l = l'$.

For the final formula: let $d = (a, b)$. Then $d = ar + bs$ for some $r, s$. Let $l = ab/d$. Since $d|a$, $l = (\frac{a}{d})b$ is an integer. From this, furthermore, we see that $b|l$. Likewise $a|l$.

Now suppose $a|m, b|m$ for some $m$. Then $m = am_1 = bm_2$. So $md = mar + mbs = bm_2ar + am_1bs = ab(m_2r + m_1s)$. Hence $m = \frac{ab}{d}(m_2r + m_1s)$. This shows that $l|m$.

**Definition 1.19.** A positive integer $p > 1$ is called a prime number iff given any integer $n$, either $p|n$ or $(p,n) = 1$.

**Lemma 1.20.** Let $p$ be a positive integer greater than $1$. Then $p$ is a prime number iff the only positive numbers dividing $p$ are 1 and $p$ itself.

**Proof.** $\Rightarrow$: Suppose $p$ is a prime number and suppose $a$ is a positive number dividing $p$. We will assume that $a$ is neither 1 nor $p$ and get a contradiction. For certainly $p$ does not divide $a$, yet $(p,a) = a \neq 1$, violating the definition above.

$\Leftarrow$: Assume that $p$ is not a prime. So there exists an integer $n$ such that $p \nmid n$ and $(p,n) = a > 1$. Then $a$ is a positive number dividing $p$ which is neither 1 nor $p$ itself.

**Proposition 1.21.** Let $p$ be a prime number and suppose $p$ divides the product of $a_1, a_2, \ldots, a_k$. Then $p$ divides one of the factors.

**Proof.** Supply a proof using induction.

The following is called the Unique Factorization Theorem and also as the Fundamental Theorem of Arithmetic.

**Unique Factorization Theorem 1.22.** Any positive integer greater than 1 can be factored into a product of one or more prime numbers and this factorization is unique up to permutations of the factors.
Proof. (Note that a product of one prime just means the prime itself.)

First we discuss the factoring. If the statement is NOT true, there is some positive integer (> 1) which cannot be factored into a product of one or more primes, and by the WOP, let \( n \) be the smallest such. We will reach a contradiction. If \( n \) is a prime, then \( n \) is a product of one prime. So \( n \) is not a prime \( ie. n \) is composite. So \( n \) has a positive divisor \( a \) which is neither 1 nor \( n \), hence \( n = ab \) where both \( a, b \) are strictly between 1 and \( n \). By our choice of \( n \), the statement is true for each of \( a, b \). Hence each of \( a, b \) is a product of one or more primes and therefore their product is also a product of primes. Contradiction.

Next we work on the uniqueness of the factoring. Again we proceed by contradiction and suppose that \( n \) is the smallest integer > 1 for which the factorization is NOT unique. So

\[
n = p_1 p_2 \ldots p_k = q_1 q_2 \ldots q_l,
\]

has two different factorizations into primes numbers. Now if \( k = 1 \), then \( l = 1 \) as well since \( n = p_1 \) cannot be factored, and then \( p_1 = q_1 \), hence the two factorizations are not different after all. So it must be that both \( k \) and \( l \) are > 1. Now \( p_1|q_1 q_2 \ldots q_l \), hence by the proposition above, \( p_1 \) divides one of the factors which we take to be \( q_1 \) since we can permute the factors. Since \( q_1 \) is a prime, we get \( p_1 = q_1 \). Dividing the equation above by \( p_1 \), we get

\[
\frac{n}{p_1} = p_2 \ldots p_k = q_2 \ldots q_l.
\]

Now \( 1 < \frac{n}{p_1} < n \), and hence by our choice of \( n \) the two factorizations of \( \frac{n}{p_1} \) must be the same up to permutations. But this tells us that the two factorizations of \( n \) are also the same up to permutations. Contradiction.

\[\Box\]

**Theorem 1.23.** Let \( a = \pm p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}, b = \pm p_1^{f_1} p_2^{f_2} \ldots p_k^{f_k} \) be prime factorizations of two non-zero integers into powers of distinct primes \( p_1, p_2, \ldots, p_k \), where we allow an exponent to be zero if that prime does not divide the integer. Then

\[
(a, b) = p_1^{\min\{e_1, f_1\}} p_2^{\min\{e_2, f_2\}} \ldots p_k^{\min\{e_k, f_k\}}.
\]

**Proof.** Hint: first use 1.12, 1.16 to show that all you really need to prove is that the gcd of \( p^e \) and \( p^f \) equals the smaller of the two numbers for any prime (or number) \( p \). \( \Box \)
A better way to calculate the gcd of two positive numbers is to use the Euclidean Algorithm. This also allows you to express the gcd as an integer linear combination of $a$ and $b$. First

**Lemma 1.24.** Given $a$ and $b = qa + r$, then $(a, b) = (a, r)$.

**Proof.** Let $d = (a, b), d' = (a, r)$, both of which are smallest positive integer linear combinations by 1.10. So $d = ax + by = a(x + qy) + ry$, a combination of $a$ and $r$. Hence $d' \leq d$. Likewise we show that $d \leq d'$. □

**Algorithm 1.25.** (Euclidean Algorithm) Given $0 < a \leq b$,

- use the division algorithm to express $b$ as
- $b = qa + r, \ 0 \leq r < a$;
- If $r = 0$, it means that $a \mid b$ and so $(a, b) = a$. Done.
- If $r \neq 0$, $(a, b) = (r, a)$ by the lemma above.
- Recursively, apply the algorithm to find $(r, a)$.

**Proof.** A proof is required to show that the algorithm terminates. Each recursive call computes a new remainder which is smaller than the previous. Hence sooner or later, a remainder must become zero. At this point, the algorithm terminates. □