1. **Definition (The Well Ordering Principle)** - Every nonempty set of positive integers contains a smallest member.

2. **Theorem (The Division Algorithm)** - Let $a$ and $b$ be integers with $b > 0$. Then there exist unique integers $q$ and $r$ with the property that $a = bq + r$, where $0 \leq r < b$.

3. **Definition** - The Greatest Common Divisor of two nonzero integers $a$ and $b$ is the largest of all common divisors of $a$ and $b$. We denote this integer by $\gcd(a, b)$. When $\gcd(a, b) = 1$, we say $a$ and $b$ are relatively prime.

4. **Theorem** For any nonzero integers $a$ and $b$, there exist integers $s$ and $t$ such that $\gcd(a, b) = as + bt$. Moreover, $\gcd(a, b)$ is the smallest positive integer of the form $as + bt$.

5. **Corollary** If $a$ and $b$ are relatively prime, then there exist integers $s$ and $t$ such that $as + bt = 1$.

6. **Theorem (Euclid’s Lemma)** If $p$ is a prime that divides $ab$, then $p$ divides $a$ or $p$ divides $b$ (or both).
   **Proof:** Suppose that $p$ is a prime that divides $ab$, but without loss of generality (WLOG) does not divide $a$. Then we must show that $p$ divides $b$. Since $p$ does not divide $a$, then $a$ and $p$ are relatively prime. So there exist integers $s$ and $t$ such that $1 = as + pt$. Multiply through by $b$ to get $b = abs + ptb$. Since $p$ divides $ab$ and $p$ divides itself, $p$ divides the right hand side of the equation. Hence $p$ divides the left as well. So $p$ divides $b$. □

7. **Theorem (Fundamental Theorem of Arithmetic)** Every integer greater than 1 is a prime or a product of primes. This product is unique, except for the order in which the factors appear. That is, if $n = p_1 p_2 \ldots p_r$ and $n = q_1 q_2 \ldots q_s$, where the $p_i$’s and $q_j$’s are primes, then $r = s$ and, after renumbering the $q_j$’s, we have $p_i = q_i$ for all $i$.

8. **Definition** The least common multiple of two nonzero integers $a$ and $b$ is the smallest positive integer that is a multiple of both $a$ and $b$. We denote this integer by $\text{lcm}(a, b)$.

9. **Theorem (The First Principle of Mathematical Induction)** Let $S$ be a set of integers containing $a$. Suppose $S$ has the property that whenever some integer $n \geq a$ belongs to $S$, then the integer $n+1$ belongs to $S$. Then $S$ contains every integer greater than or equal to $a$.

10. **Theorem (DeMoivre’s Theorem)** For every positive integer $n$ and every real number $\theta$, $(\cos \theta + i \sin \theta)^n = \cos n\theta + i \sin n\theta$, where $i$ is the complex number $\sqrt{-1}$.
    **Proof:** Base Step: The statement is clearly true for $n = 1$.
    Inductive Step: Assume true for $n$. Show the statement is true for $n+1$. In other words, assume $(\cos \theta + i \sin \theta)^n = \cos n\theta + i \sin n\theta$, prove $(\cos \theta + i \sin \theta)^{n+1} = \cos (n+1)\theta + i \sin (n+1)\theta$.
    We see that
    \[
    (\cos \theta + i \sin \theta)^{n+1} = (\cos \theta + i \sin \theta)^n (\cos \theta + i \sin \theta)
    = (\cos n\theta + i \sin n\theta)(\cos \theta + i \sin \theta)
    = \cos n\theta \cos \theta + i (\sin n\theta \cos \theta + \sin \theta \cos n\theta) - \sin n\theta \sin \theta.
    \]
    Now, using trig identities for $\cos(\alpha + \beta)$ and $\sin(\alpha + \beta)$, we see that this last term is $\cos(n+1)\theta + i \sin(n+1)\theta$. So, by induction, the statement is true for all positive integers. □

11. **Theorem (The Second (Strong) Principle of Mathematical Induction)** Let $S$ be a set of integers containing $a$. Suppose $S$ has the property that $n$ belongs to $S$ whenever every integer less than $n$ and greater than or equal to $a$ belongs to $S$. Then $S$ contains every integer greater than or equal to $a$.
12. **Definition** An *equivalence relation* on a set $S$ is a set $R$ of ordered pairs of elements of $S$ such that

   (a) $(a,a) \in R$ for all $a \in S$. (reflexive property)
   (b) $(a,b) \in R$ implies $(b,a) \in R$ (symmetric property)
   (c) $(a,b) \in R$ and $(b,c) \in R$ imply $(a,c) \in R$ (transitive property)

13. **Definition** A *partition* of a set $S$ is a collection of nonempty disjoint subsets of $S$ whose union is $S$.

14. **Theorem** The equivalence classes of an equivalence relation on a set $S$ constitute a partition of $S$. Conversely, for any partition $P$ of $S$, there is an equivalence relation on $S$ whose equivalence classes are the elements of $P$. 