Basics

Well Ordering Principle And Division Algorithm

Well Ordering Principle: Every nonempty set of positive integers contains a smallest member. (*Take is as an axiom*)

Theorem 1.1 (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 $0 \leq r < b$.

Proof: We begin with the existence portion of the theorem. Consider the set $S =$
$a - bk \mid k$ is an integer and $a - bk \geq 0$. If $0 \in S$, then b divides a and we may obtain the desired result with $q = a/b$ and $r = 0$. Now assume $0 \notin S$. Since S is nonempty [if $a > 0, a - b.0 \in S$; if $a < 0, a - b(2a) = a(1 - 2b) \in S$; $a \neq 0$ since $0 \notin S$], we may apply the Well Ordering Principle to conclude that S has a smallest member, say $r = a - bq$. Then $a = bq + r$ and $r \geq 0$, so all that remains to be proved is that $r < b$. If $r \geq b$, then $a - b(q + 1) = a - bq - b = r - b \geq 0$, so that $a - b(q + 1) \in S$. But $a - b(q + 1) < a - bq$, and $a - bq$ is the smallest member of S. So, $r < b$. To establish the uniqueness of q and r, let us suppose that there are integers q, q', r, and r' such that $a = bq + r, 0 \leq r < b$, and $a = bq' + r', 0 \leq r' < b$. For convenience, we may also suppose that $r' \geq r$. Then $bq + r = bq' + r'$ and $b(q - q') = r' - r$. So, b divides $r' - r$ and $0 \leq r' - r \leq r' < b$. It follows that $r' - r = 0$, and therefore $r' = r$ and $q' = q$. ∎

GCD

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.

Theorem 1.2 (GCD is a linear combination): 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 $as + bt$.

Proof: Consider the set $S =$
$am + bn \mid m, n$ are integers and $am + bn > 0$. Since S is obviously nonempty (if some choice of m and n makes $am + bn < 0$, then replace m and n by $-m$ and $-n$), the Well Ordering Principle asserts that S has a smallest member, say, $d = as + bt$. We claim that $d = gcd(a, b)$. To verify this claim, use the division algorithm to write $a = dq + r$, where $0 \leq r < d$. If $r > 0$, then $r = a - dq = a - (as + bt)q = a - asq - btq = a(1 - sq) + b(-tq) \in S$, contradicting the fact that d is the smallest member of S *(Note that we wanted to show $a - dq < d$ which is obviously true as $r < d$.)*. So, $r = 0$ and d divides a. Analogously (or, better yet, by symmetry), d divides b as well. This proves that d is a common divisor of a and b. Now suppose d' is another common divisor of a and b and write $a = d'h$ and $b = d'k$. Then $d = as + bt = (d'h)s + (d'k)t = d'(hs + kt)$, so that d' is a divisor of d. Thus, among all common divisors of a and b, d is the greatest.

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

Theorem 1.3 (Euclid's Lemma): If p is a prime that divides ab, then p divides a or p divides b. (easy to see)

Fundamental theorem of arithmetic (*to be proved later*): 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.

LCM

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.

Modulo Arithmetic

When $a = qn + r$, where q is the quotient and r is the remainder upon dividing a by n, we write $a \bmod n = r$.

In general, if a and b are integers and n is a positive integer, then $a \bmod n = b \bmod n$ if and only if n divides $a - b$. (easy to see)

Examples:

- $-2 \bmod 15 = 13$ since $-2 = (-1)15 + 13$.
- Consider the statement, "The sum of the cubes of any three consecutive integers is divisible by 9." This statement is equivalent to checking that the equation $(n^3 + (n+1)^3 + (n+2)^3) \bmod 9 = 0$ is true for all integers n. Because of properties of modular arithmetic, to prove this, all we need do is check the validity of the equation for $n = 0, 1, \ldots, 8$.
- We use mod 3 arithmetic to show that there are no integers a and b such that $a^2 - 6b = 2$. To see this, suppose that there are such integers. Then, taking both sides modulo 3, there is an integer solution to $a^2 \bmod 3 = 2$. But trying $a = 0, 1$, and 2 we obtain a contradiction.

Mathematical Induction

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 $n + 1$ also belongs to S. Then, S contains every integer greater than or equal to a.

Second 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.

Examples:

- We will use the Second Principle of Mathematical Induction with $a = 2$ to prove the existence portion of the Fundamental Theorem of Arithmetic. Let S be the set of integers greater than 1 that are primes or products of primes. Clearly, $2 \in S$. Now we assume that for some integer n, S contains all integers k with $2 \leq k < n$. We must show that $n \in S$. If n is a prime, then $n \in S$ by definition. If n is not a prime, then n can be written in the form ab, where $1 < a < n$ and $1 < b < n$. Since we are assuming that both a and b belong to S, we know that each of them is a prime or a product of primes. Thus, n is also a product of primes. This completes the proof. ■
- The Quakertown Poker Club plays with blue chips worth \$5.00 and red chips worth \$8.00. What is the largest bet that cannot be made?

To gain insight into this problem, we try various combinations of blue and red chips and obtain 5, 8, 10, 13, 15, 16, 18, 20, 21, 23, 24, 25, 26, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40. It appears that the answer is 27. But how can we be sure? Well, we need only prove that every integer greater than 27 can be written in the form $a*5+b*8$, where a and b are nonnegative integers. This will solve the problem, since a represents the number of blue chips and b the number of red chips needed to make a bet of $a*5+b*8$. For the purpose of contrast, we will give two proofs—one using the First Principle of Mathematical Induction and one using the Second Principle. Let S be the set of all integers greater than or equal to 28 of the form $a*5+b*8$, where a and b are nonnegative. Obviously, $28 \in S$. Now assume that some integer $n \in S$, say, $n = a*5+b*8$. We must show that $n+1 \in S$. First, note that since $n \geq 28$, we cannot have both a and b less than 3. If $a \geq 3$, then $n+1 = (a*5+b*8)+(-3*5+2*8) = (a-3)*5+(b+2)*8$. If $b \geq 3$, then $n+1 = (a*5+b*8)+(5*5-3*8) = (a+5)*5+(b-3)*8$. This completes the proof. To prove the same statement by the Second Principle, we note that each of the integers 28, 29, 30, 31, and 32 is in S. Now assume that for some integer $n > 32$, S contains all integers k with $28 \leq k < n$. We must show that $n \in S$. Since $n-5 \in S$, there are nonnegative integers a and b such that $n-5 = a*5+b*8$. But then $n = (a+1)*5+b*8$. Thus n is in S.

Equivalence Relation

An equivalence relation on a set S is a set R of ordered pairs of elements of S such that

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

When R is an equivalence relation on a set S, it is customary to write aRb instead of $(a, b) \in R$

If $\sim$ is an equivalence relation on a set S and $a \in S$, then the set $[a] =$
$x \in S \mid x \sim a$ is called the equivalence class of S containing a.

Examples:

- Let S be the set of integers and let n be a positive integer. If $a, b \in S$, define $a \equiv b$ if $a \bmod n = b \bmod n$ (that is, if $a-b$ is divisible by n). Then $\equiv$ is an equivalence relation on S and $[a] =$
$a + kn \mid k \in S$.

Partition

A partition of a set S is a collection of nonempty disjoint subsets of S whose union is S.

Theorem 1.4: 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 . (First part is easy, for second part, Define $a \sim b$ if a and b belong to the same subset in the collection.)

Functions

Definition: A function (or mapping) ϕ from a set A to a set B is a rule that assigns to each element a of A exactly one element b of B.

Definition: Let $\phi : A \rightarrow B$ and $\psi : B \rightarrow C$. The composition $\psi\phi$ is the mapping from A to C defined by $(\psi\phi)(a) = \psi(\phi(a))$ for all a in A .

Definition: A function f from a set A is called one-to-one if for every $a_1, a_2 \in A, f(a_1) = f(a_2)$ implies $a1 = a2$.

Alternatively f is one-to-one if $a1 \neq a2$ implies $f(a_1) \neq f(a_2)$

Definition: In symbols, $\phi : A \rightarrow B$ is onto if for each b in B there is at least one a in A such that $\phi(a) = b$.

Properties

Given functions $\alpha : A \rightarrow B, \beta : B \rightarrow C$, and $\gamma : C \rightarrow D$, then

1. $\gamma(\beta\alpha) = (\gamma\beta)\alpha$ (associativity).
2. If α and β are one-to-one, then $\beta\alpha$ is one-to-one.
3. If α and β are onto, then $\beta\alpha$ is onto.
4. If α is one-to-one and onto, then there is a function α^{-1} from B onto A such that $\left(\alpha^{-1}\alpha\right)(a) = a$ for all a in A and $\left(\alpha\alpha^{-1}\right)(b) = b$ for all b in B .

Proof:

1. Let $a \in A$. Then $(\gamma(\beta\alpha))(a) = \gamma((\beta\alpha)(a)) = \gamma(\beta(\alpha(a)))$. On the other hand, $((\gamma\beta)\alpha)(a) = (\gamma\beta)(\alpha(a)) = \gamma(\beta(\alpha(a)))$. So , $\gamma(\beta\alpha) = (\gamma\beta)\alpha$
2. Easy
3. Easy
4. Easy
